MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

SMART CITIES IN DARKNET ERA

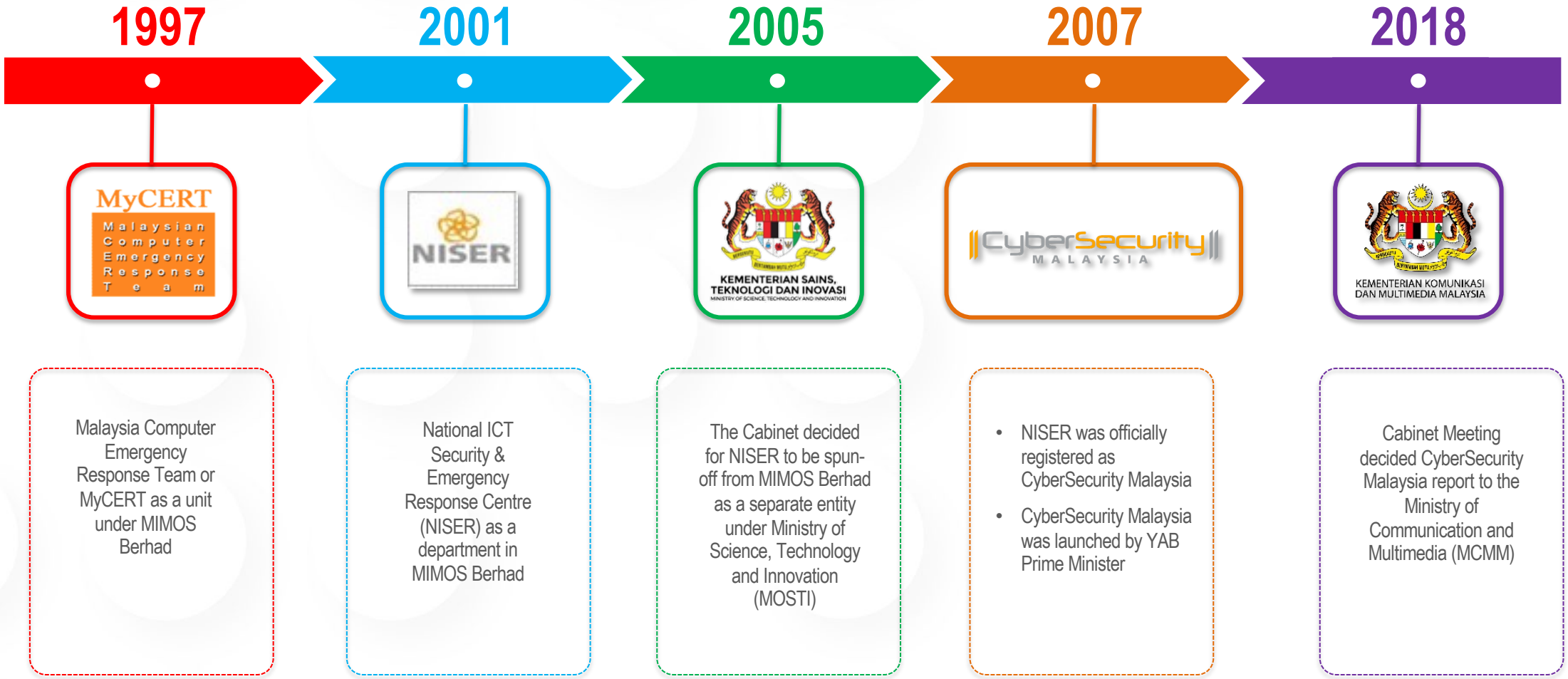
"SMART CITIES, DARKNET RESILIENCE REQUIRED "

Nurshahira Binti Mohd,
Cyber Risk Intelligence Department

SECURING
OUR
CYBERSPACE

Copyright © 2023 CyberSecurity Malaysia

History Timelines



Copyright © 2023 CyberSecurity Malaysia

Visi dan Misi CyberSecurity Malaysia

VISION

World-class cyber security specialist agency

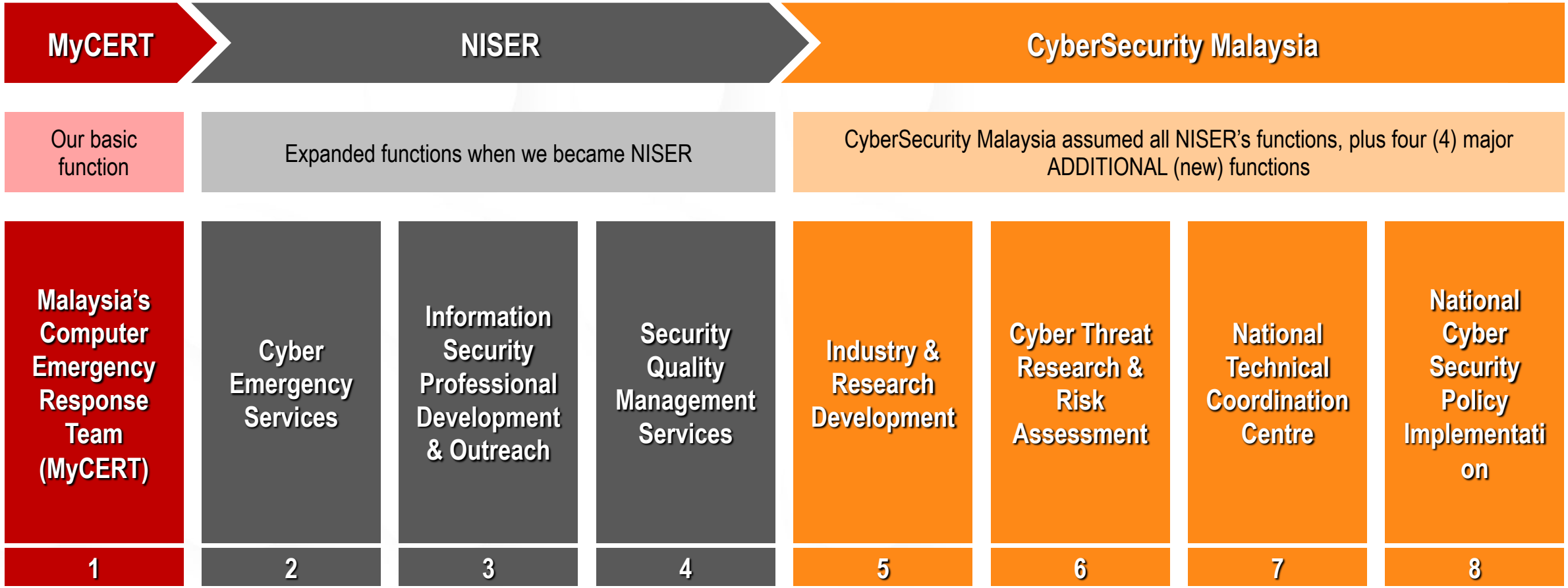
MISSION

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity and social harmony through

- Provision of quality and impactful services
- Frontier-expanding cyber knowledge and technical supremacy
- Continuous nurturing of talent and expertise

Copyright © 2023 CyberSecurity Malaysia

Our Functions



Copyright © 2023 CyberSecurity Malaysia

Cyber Risk Intelligence - Services

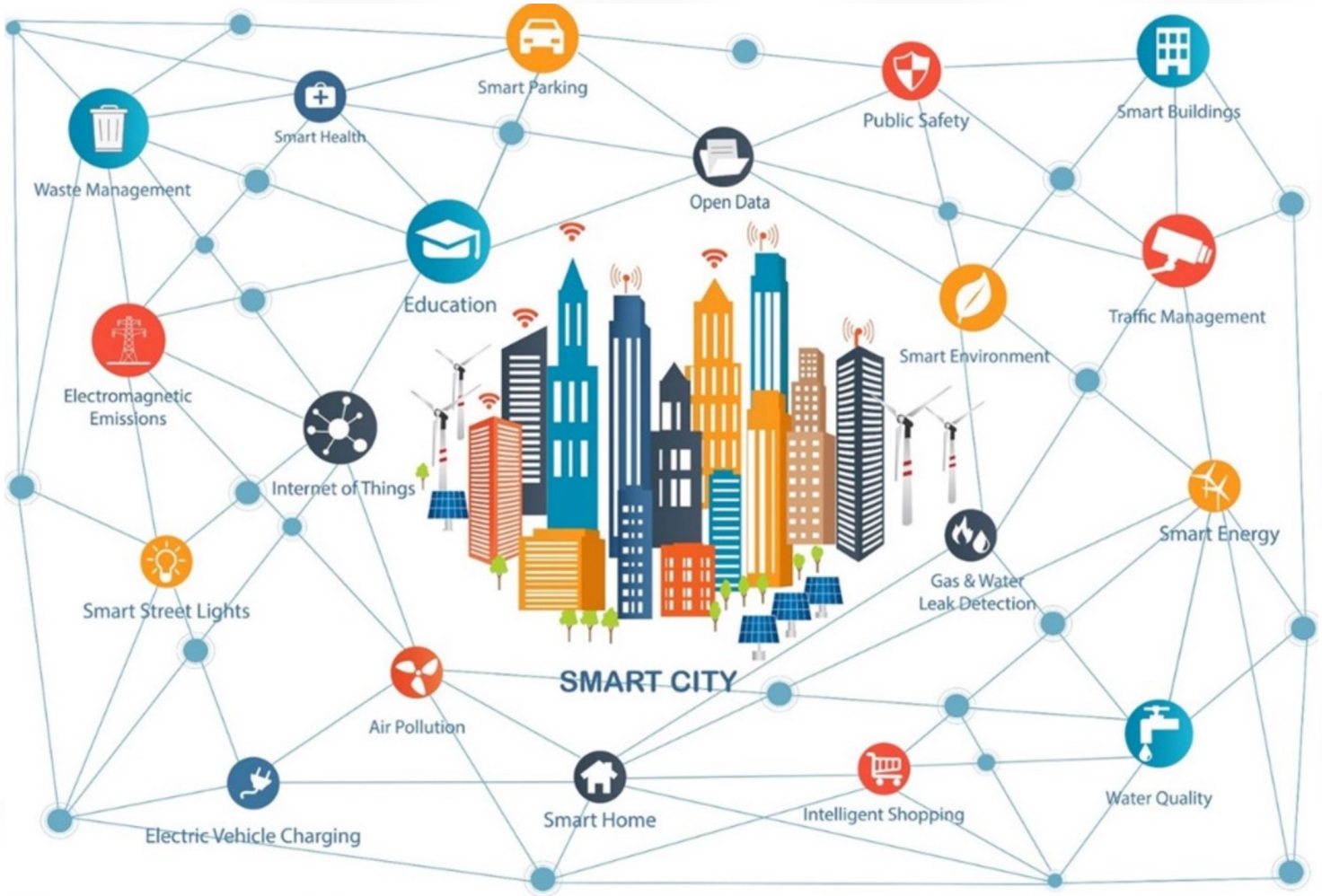
DARKWEB OPERATIONAL INTELLIGENCE

ATTACK SURFACE MANAGEMENT

NETWORK DEFENCE MONITORINNG

Copyright © 2023 CyberSecurity Malaysia

SMART CITIES IN CYBERSECURITY



A smart city is an urban environment that leverages technology to enhance the efficiency of various systems and improve the quality of life for its inhabitants. Through interconnected devices, data collection, and analysis, a smart city optimizes services like transportation, energy, healthcare, and security, fostering a more sustainable and responsive urban ecosystem.

Copyright © 2023 CyberSecurity Malaysia

SMART CITY & THREATS & DARKWEB

SMART CITY

Smart cities, with their interconnected systems and reliance on data, bring about numerous advantages but also introduce risks, particularly in the realm of data security:

- **Data Breaches**
- **Cyberattacks on Infrastructure**
- **IoT Device Vulnerabilities**
- **Human Error**
- **Social Engineering Attacks**

Copyright © 2023 CyberSecurity Malaysia

SMART CITY & THREATS & DARKWEB

THREAT

System Vulnerability

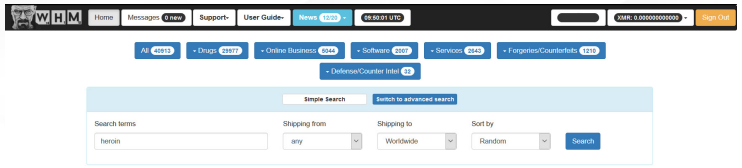
Malware

Hacker/APT/Hacktivist

Human Error

Copyright © 2023 CyberSecurity Malaysia

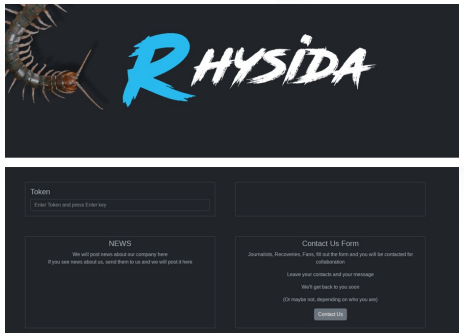
SMART CITY & THREATS & DARKWEB



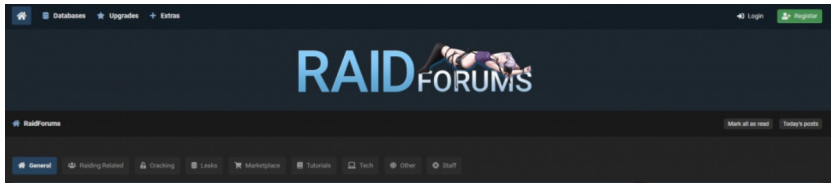
FINANCING AND FRAUD

DARKNET MARKET

Darkweb



RANSOMWARE

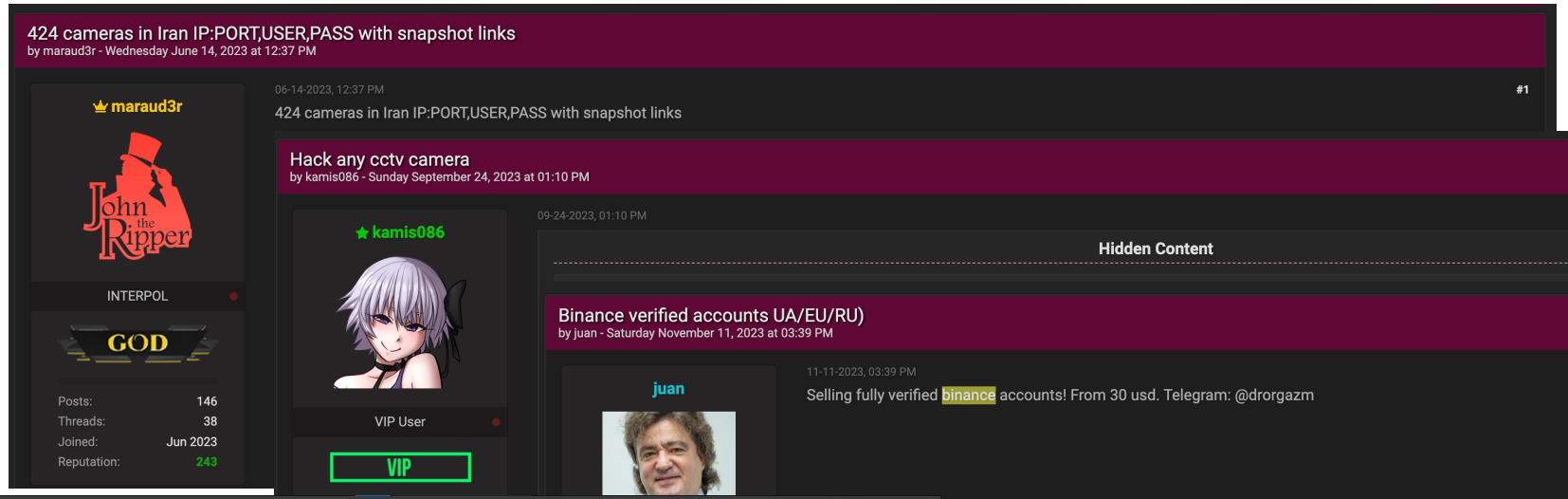


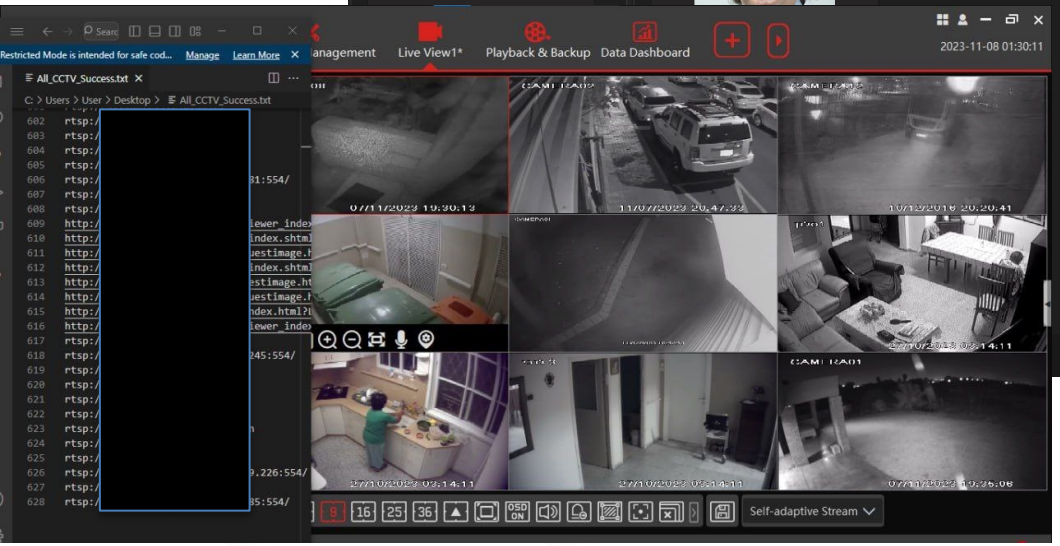
HACKING FORUM

BITCOIN SERVICE

Copyright © 2023 CyberSecurity Malaysia

SMART CITY & THREATS & DARKWEB





Florida bar America state cctv hacked by Ganosecteam

http[redacted]

Copyright © 2023 CyberSecurity Malaysia

SMART CITY & THREATS & DARKWEB

THREATS

SMART CITY

DARKWEB

Darknet as a Destination for Stolen Smart City Data
Potential Risks Arising from Data on Darknet
Securing Smart City Data

Copyright © 2023 CyberSecurity Malaysia

Who owns the personal data of Malaysians?

Copyright © 2023 CyberSecurity Malaysia

PERSONAL DATA PROTECTION ACT 2010 (PDPA) OF ACT 709.

JABATAN PERLINDUNGAN DATA PERIBADI

Kementerian Komunikasi dan Multimedia Malaysia

Copyright © 2023 CyberSecurity Malaysia

PRINCIPAL PARTY UNDER ACT 709

DATA USERS

Individuals or companies that process personal data in commercial transactions

DATA PROCESSOR

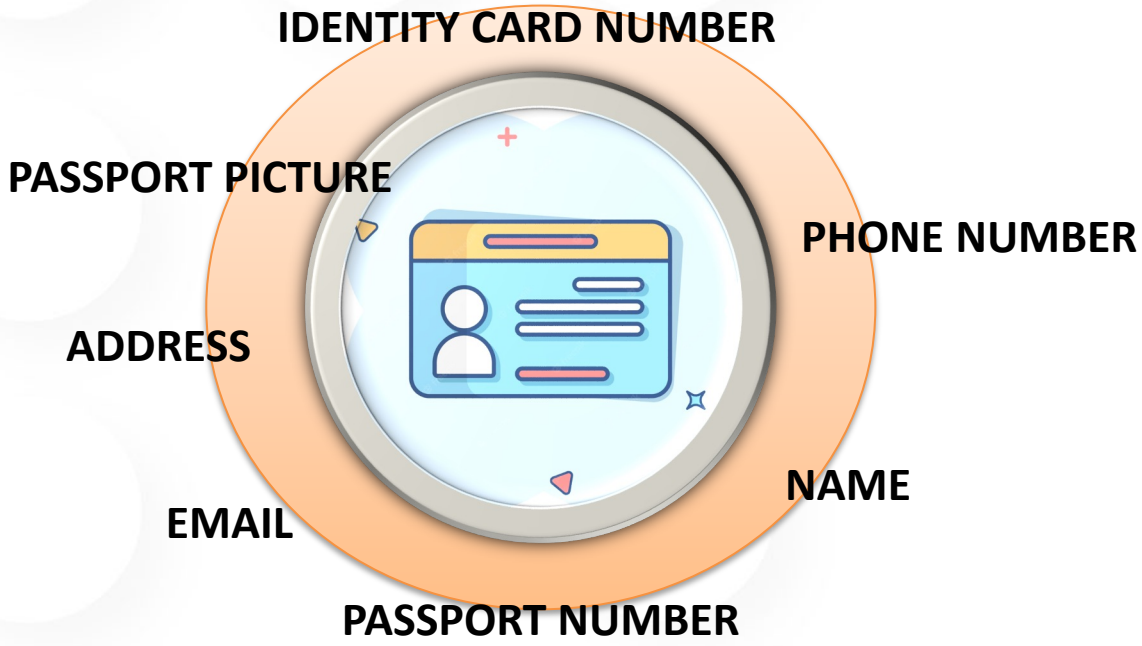
Individuals or companies that process personal data on behalf of data users

DATA SUBJECT

Owner of personal data Ex:Employees or Customers

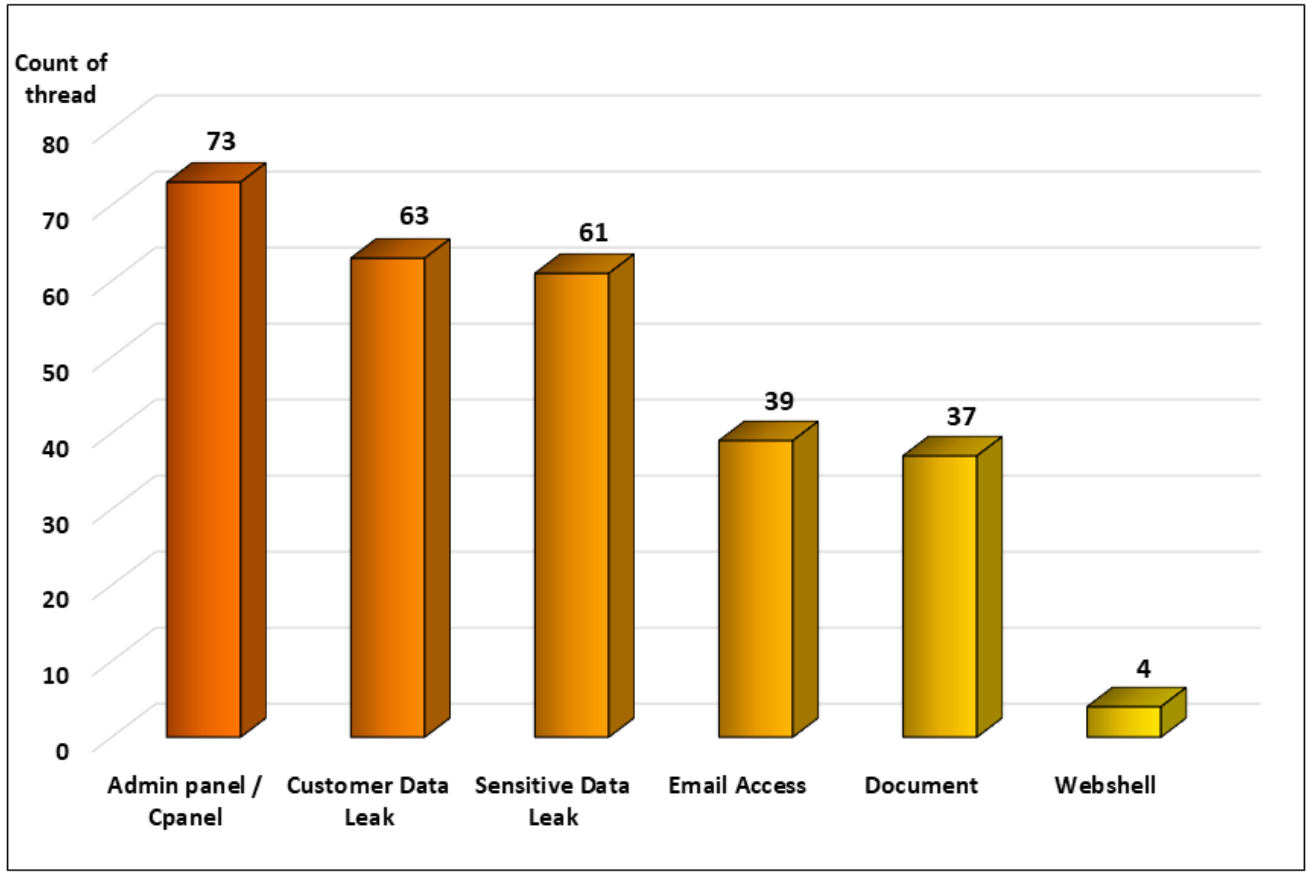
Copyright © 2023 CyberSecurity Malaysia

PERSONAL IDENTIFIABLE INFORMATION



Copyright © 2023 CyberSecurity Malaysia

STATISTIC TYPE OF DATA LEAKAGE



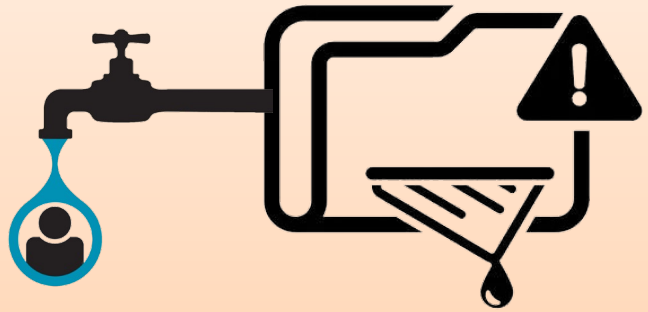
Copyright © 2023 CyberSecurity Malaysia

DATA BREACH VS DATA LEAK

DATA BREACH

A data breach occurs as a result of a security incident or when cybercriminals bypass security controls or launch a successful attack on systems.

VS

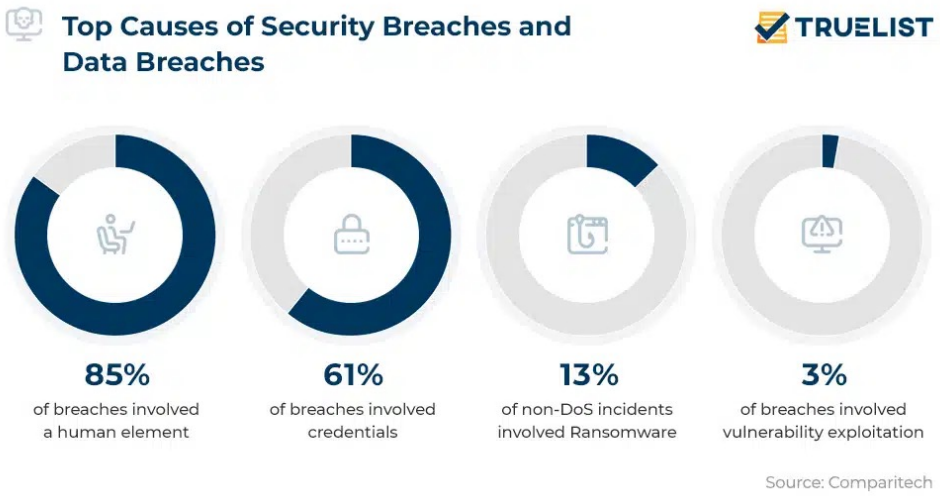


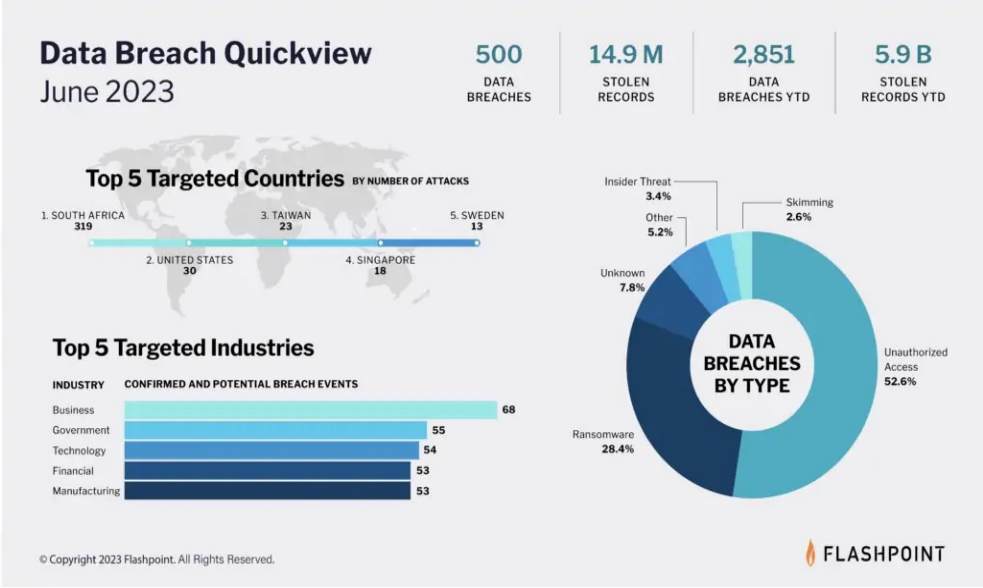
DATA LEAKAGE

Data leaks happen due to missing controls and protection.

Copyright © 2023 CyberSecurity Malaysia

CAUSES OF DATA LEAK & BREACH





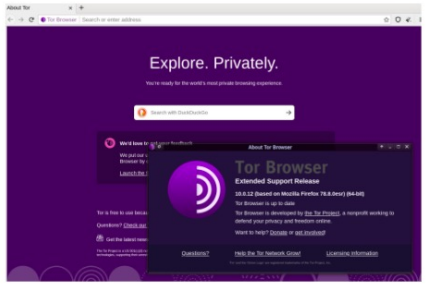
1. Insider Threat
2. Phishing Attacks
3. Malware And Ransomware
4. Weak Authentication And Authorization
5. Insecure Data Storage
6. Third-party Vulnerabilities
7. Social Engineering
8. Human Error

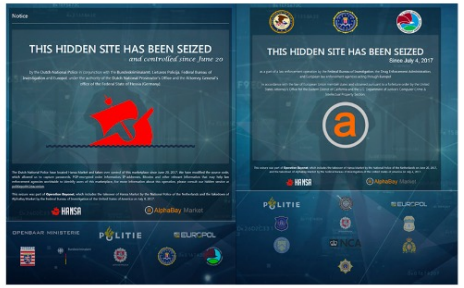
Copyright © 2023 CyberSecurity Malaysia

CAUSES OF DATA LEAK

Copyright © 2023 CyberSecurity Malaysia

HISTORY OF DARK-WEB





1980s-1990s

ORIGINS OF ANONYMITY

2002

TOR NETWORK LAUNCH

2017

DARKNET MARKET TAKEDOWNS

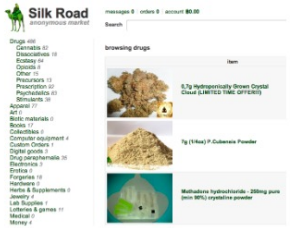
1990s

THE ONION ROUTING PROJECT

TorProject.org

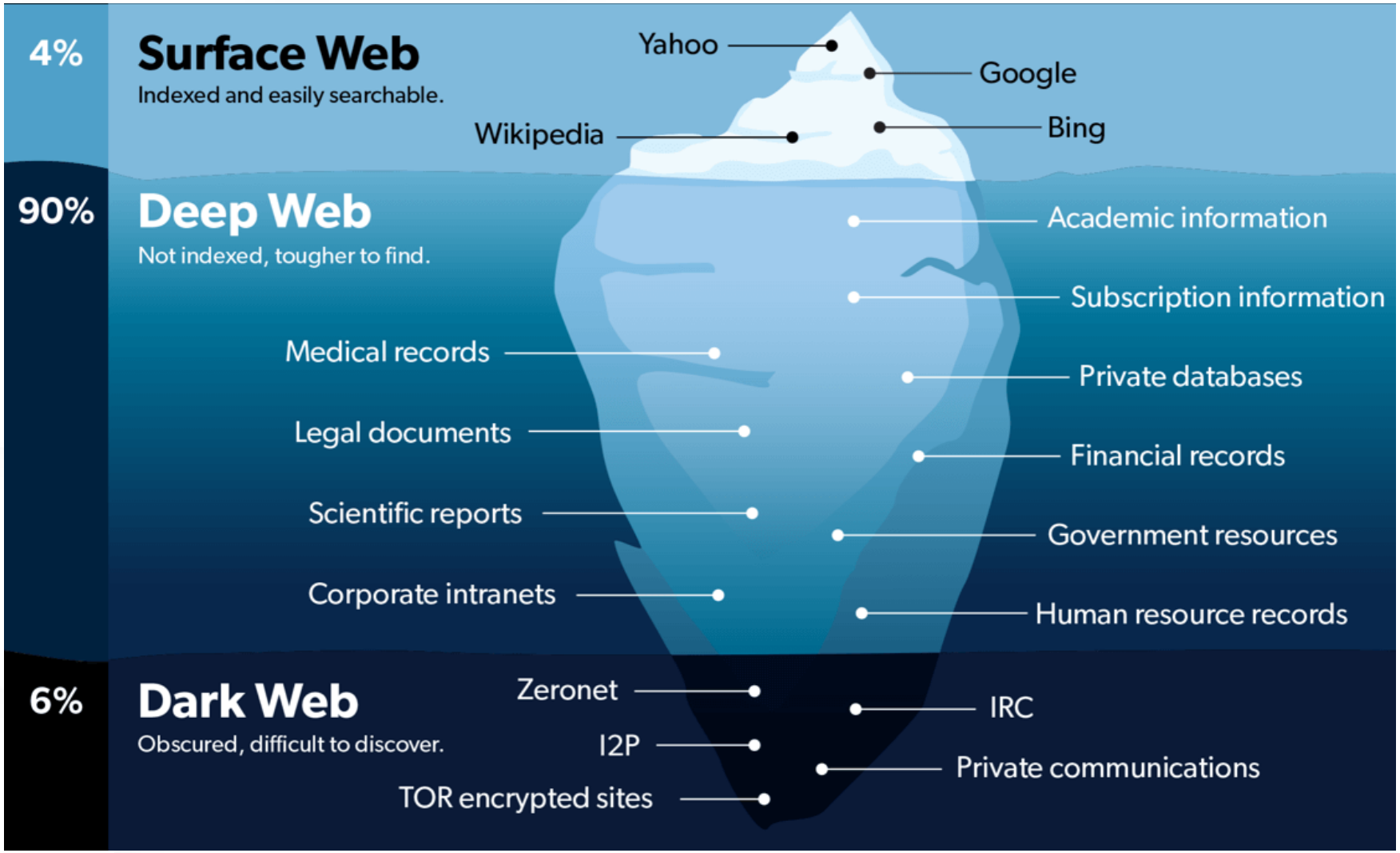
2011

SILK ROAD



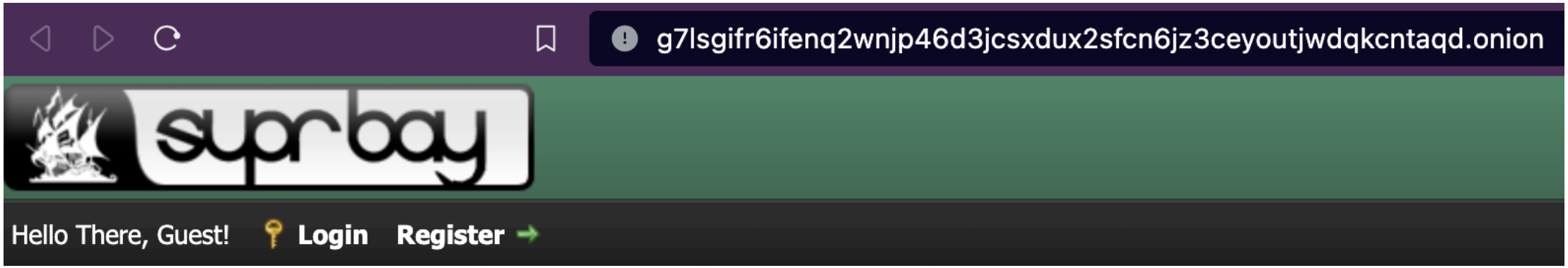
Copyright © 2023 CyberSecurity Malaysia

WHAT IS DARK-WEB



Copyright © 2023 CyberSecurity Malaysia

WHAT IS DARK-WEB



DARKWEB URL CHARACTERISTIC:

1. Some of them are very long
2. Random combinations of letters and numbers
3. Ended with .onion top-level domain names.

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion

http://pqqmr3p3tppwqvvapi6fa7jowrehgd36c56lzr26qqormaqvh6gt4jyd.onion

http://hydraclubbioknikokex7njhwuahc2l57lfiz7z36md2jvopda7nchid.onion

http://tmglsdds6usxqsghympkjfbddume3olbvpqdrpxvcxplhd4z7bxucdid.onion

http://mlyusr6htlxsyc7t2f5z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion

http://asap2u4pvplnkzl7ecle45wajojnftja44wvovl3jrvhangeyq67ziid.onion

http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion

http://rrlm2f22lpqgfhyydqkxxzv6snw55qvc2krjt2q557l7z4te7fsvhbid.onion

Copyright © 2023 CyberSecurity Malaysia

ACTIVITY IN DARK-WEB

RANSOMWARE

FINANCING AND FRAUD

DARKNET MARKET

HACKING FORUM

ILLEGAL PORNOGRAPHY

SOCIAL MEDIA

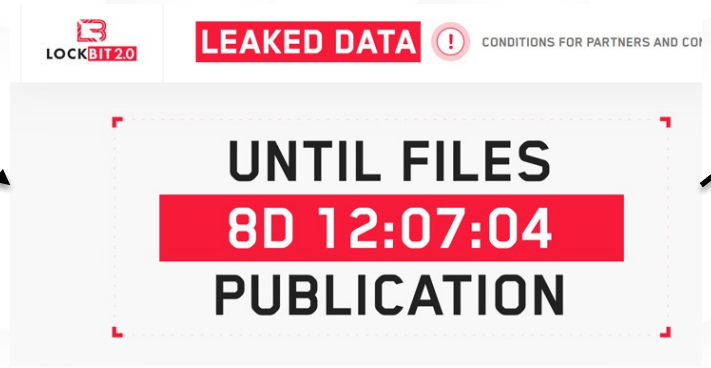
BITCOIN SERVICE

Copyright © 2023 CyberSecurity Malaysia

RANSOMWARE

RANSOMWARE

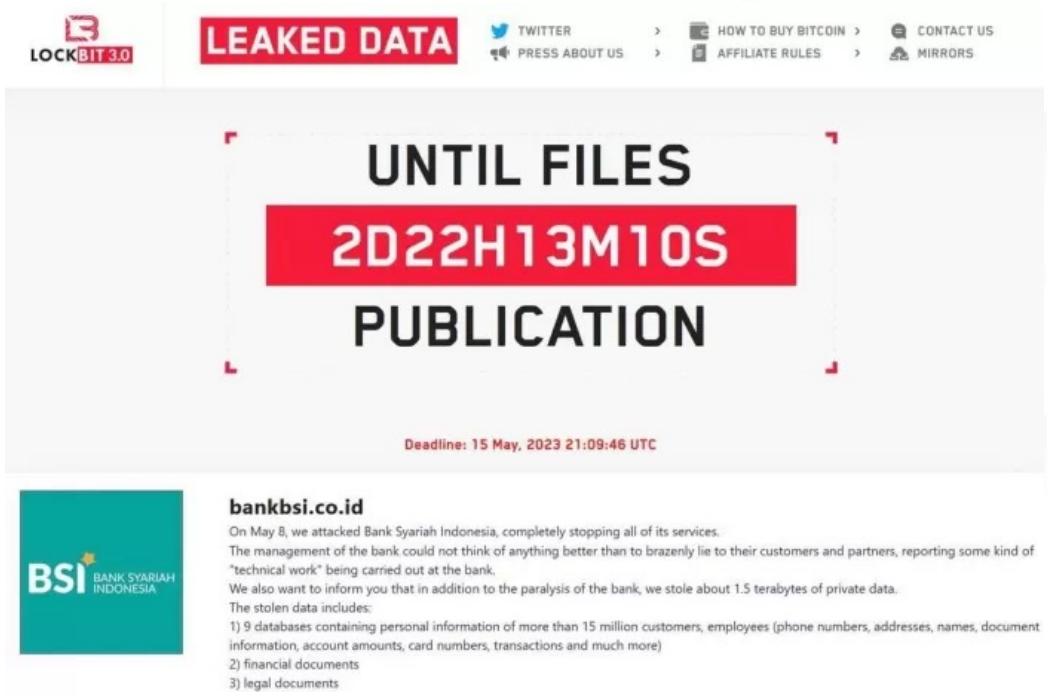
METHOD

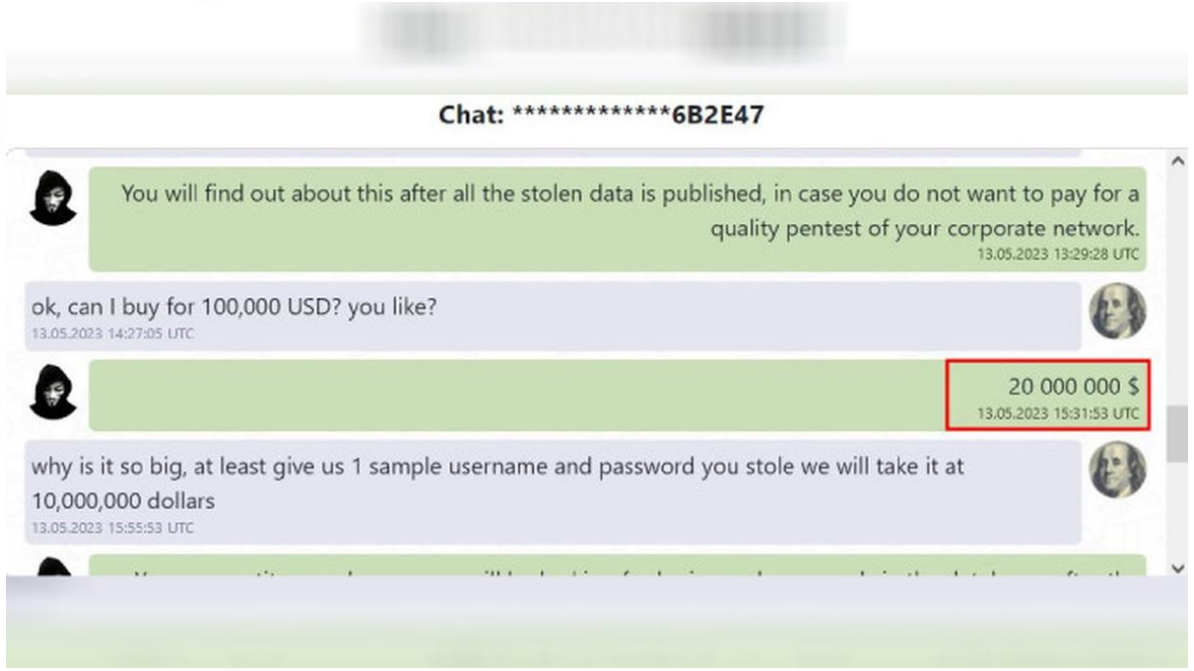


MOTIVATION

Copyright © 2023 CyberSecurity Malaysia

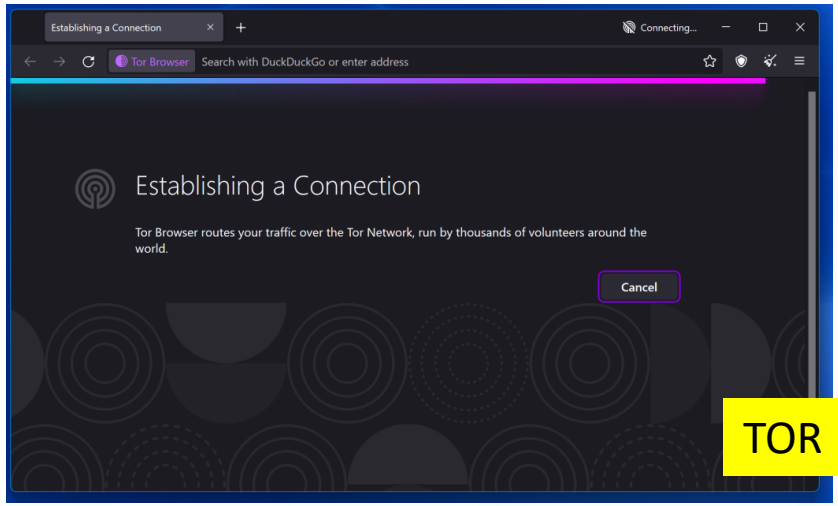
RANSOMWARE INCIDENT



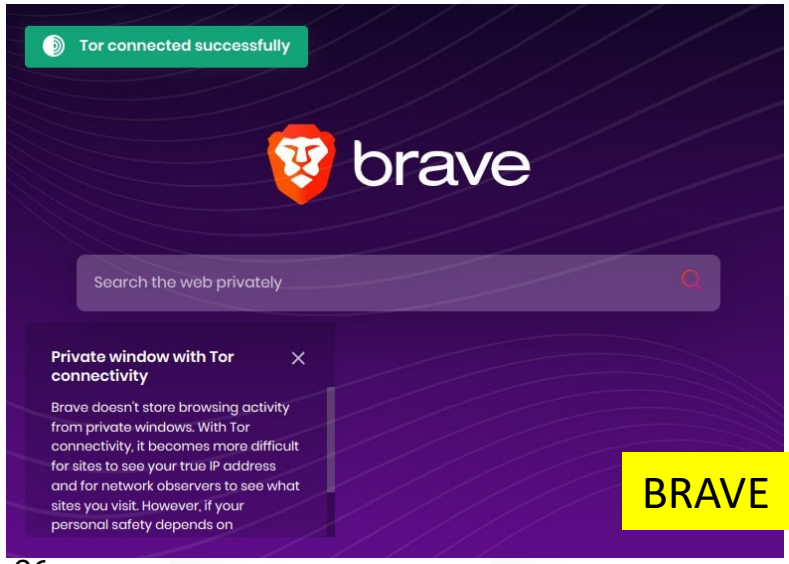


Copyright © 2023 CyberSecurity Malaysia

ACCESS DARKWEB

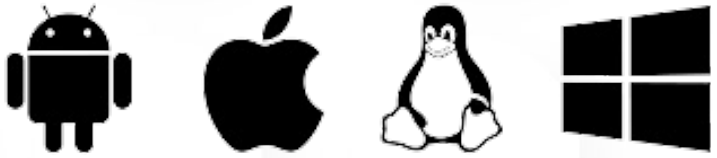


TOR



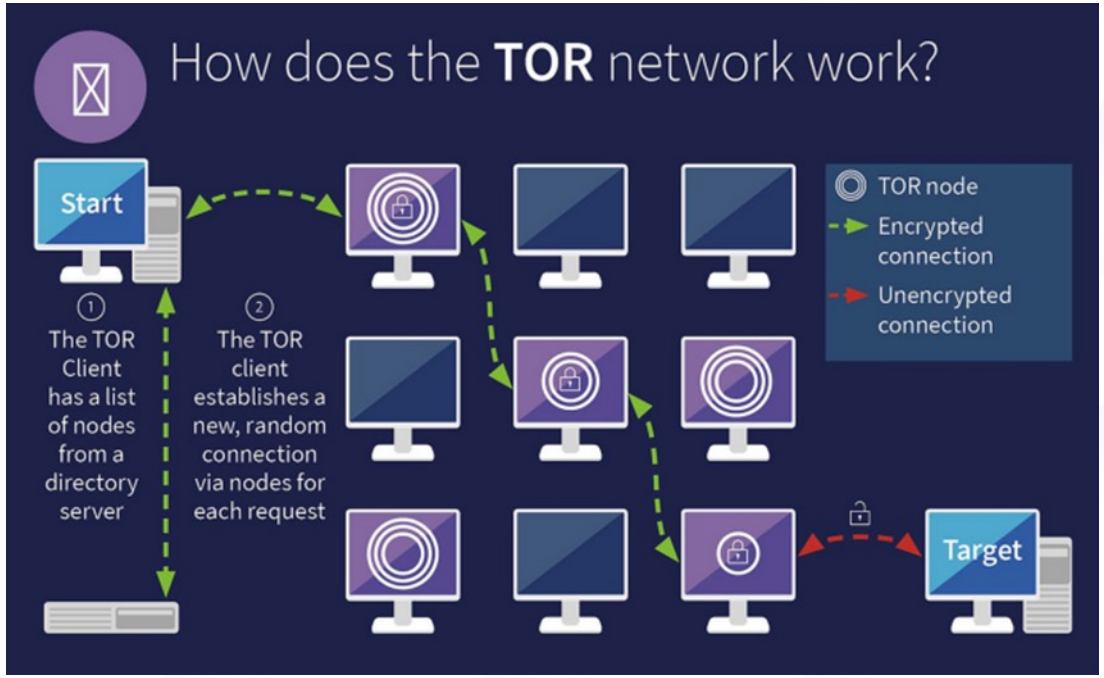
BRAVE

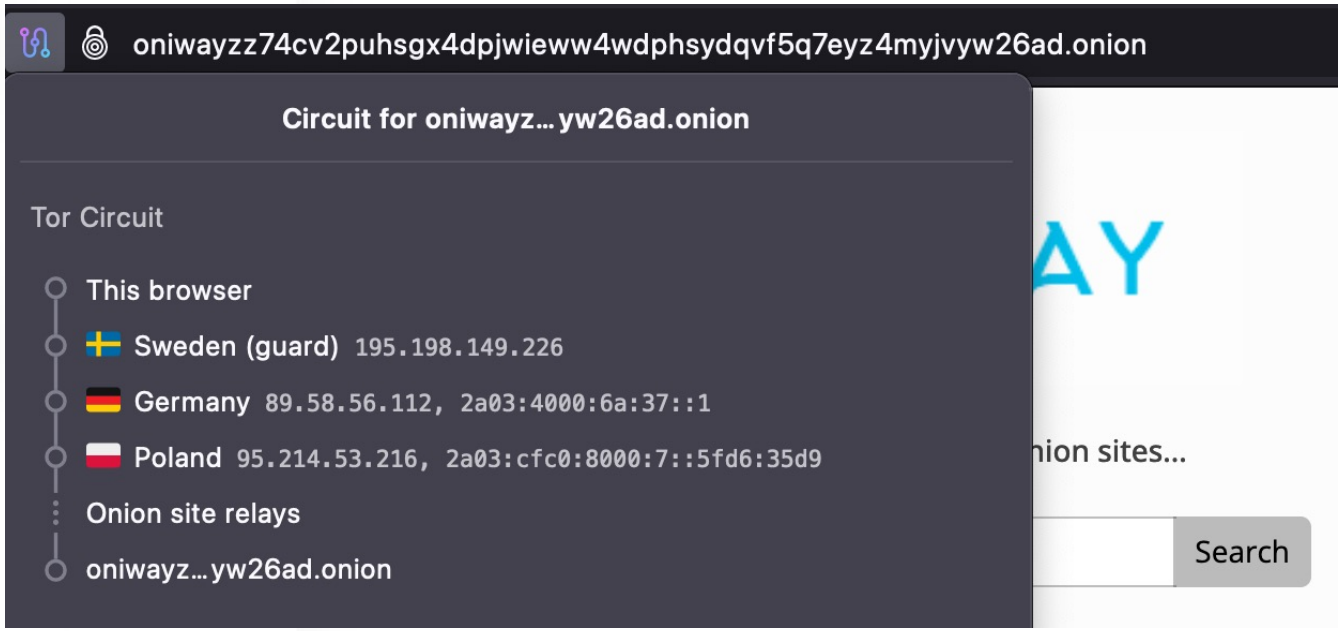
WHERE IS THE RISK



Copyright © 2023 CyberSecurity Malaysia

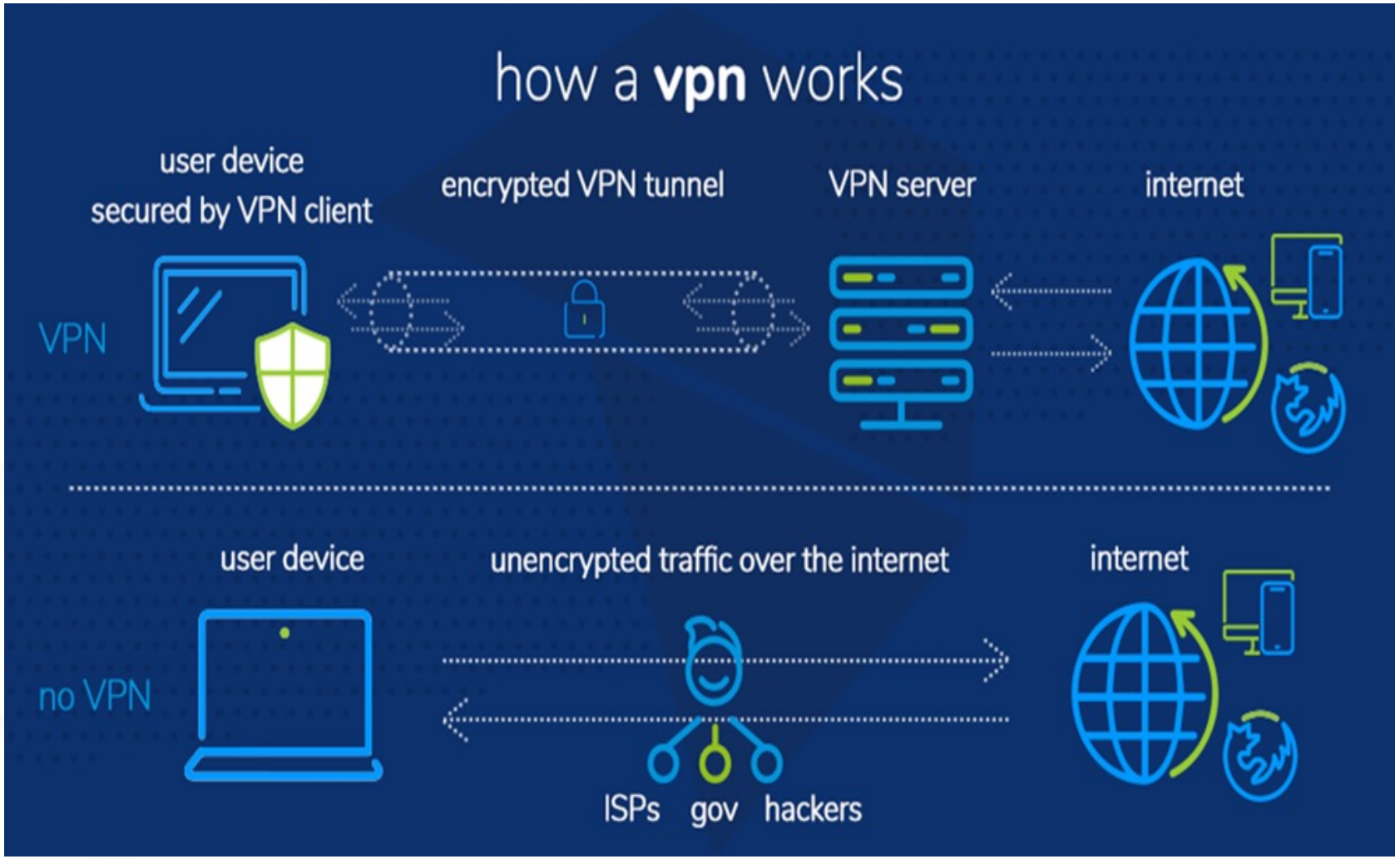
Tor Network





Copyright © 2023 CyberSecurity Malaysia

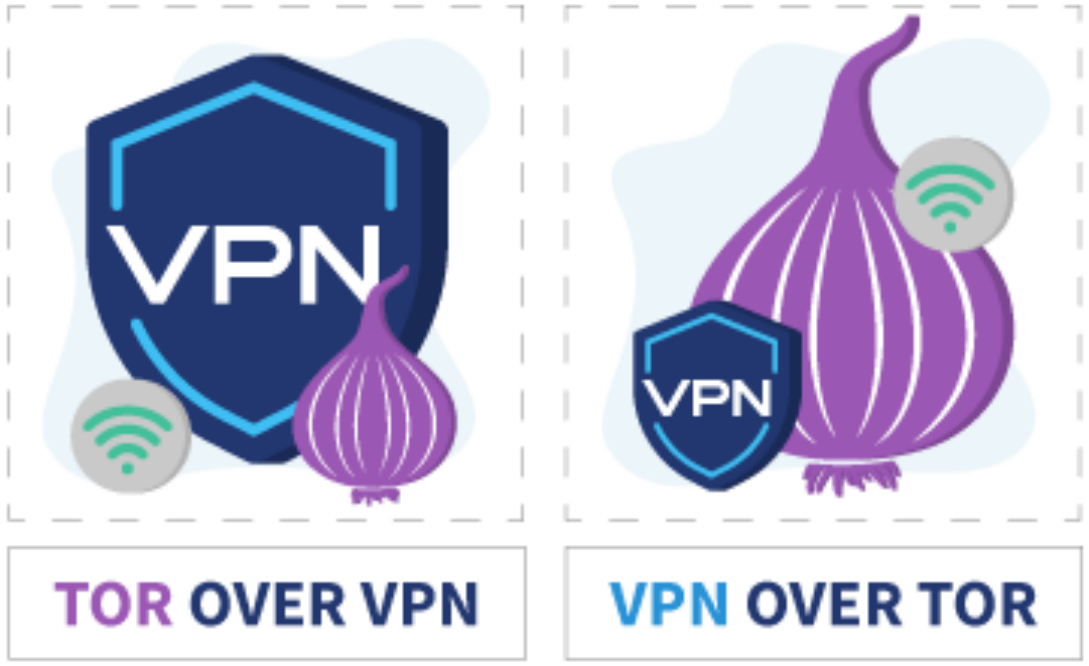
Tor Network



Copyright © 2023 CyberSecurity Malaysia

BEING ANONYMOUS

- ✓ Tails os
- ✓ Tor Browser
- ✓ Hotspot WiFi
- ✓ VPN
- ✓ Proxy
- ✓ OpenPGP
- ✓ Bitcoin
- ✓ Non-Personal Laptop
- ✓ Never shared information



Copyright © 2023 CyberSecurity Malaysia

DARKWEB TOUR

DARKWEB URL

SOCIAL MEDIA
- Reddit - https://www.reddittorjg6rue252oqsxryoxengawnmo46qy4kyii5wtqnwfj4ooad.onion
- Facebook - https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion

EMAIL
- Mail2Tor - http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion
- Onion Mail - http://pflujznptk5lmuf6xwadfqy6nffykdvahfbljh7liljailjbxrgvhfid.onion

NEWS
- Tor Times - http://tortimeswqlzti2aqbjoieisne4ubyuoeiiugel2layyudcfrwln76qd.onion

SEARCH ENGINE
- Haystak - http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion

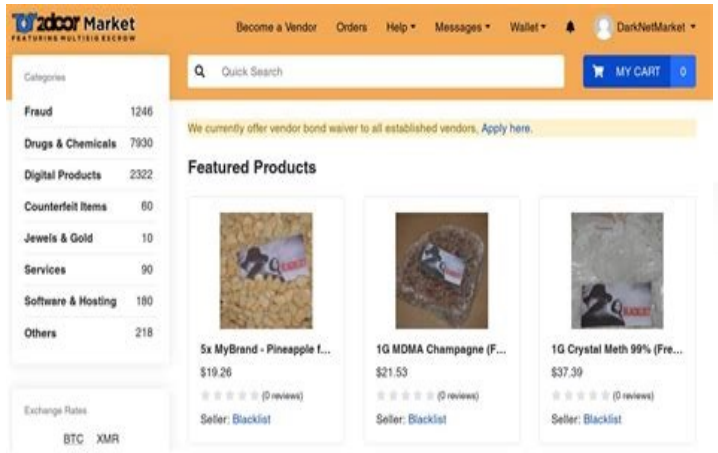
USE AT YOUR OWN RISK

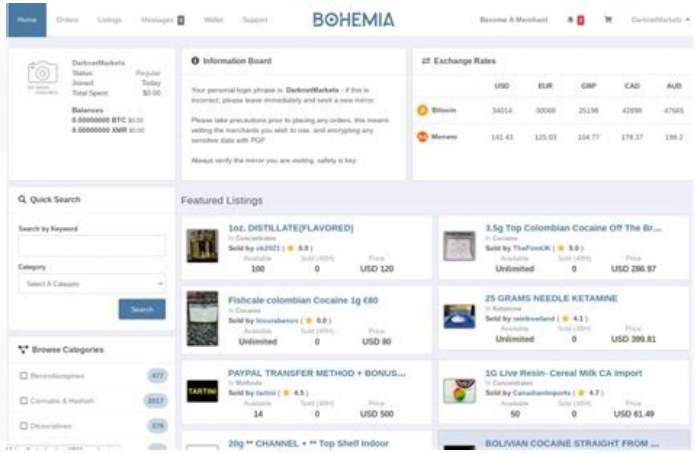
Copyright © 2023 CyberSecurity Malaysia

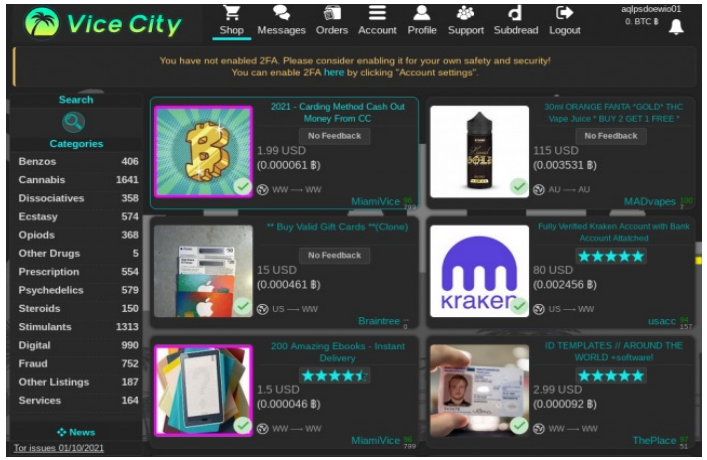
UNDERGROUND FORUM/MARKET

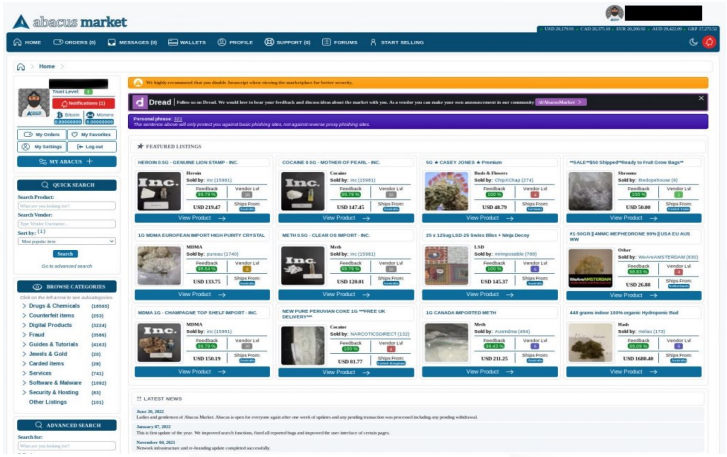
BF

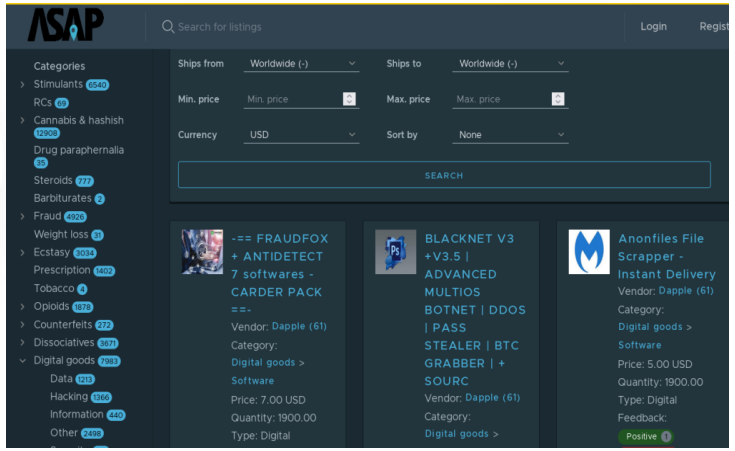
UNDERGROUND FORUM/MARKET

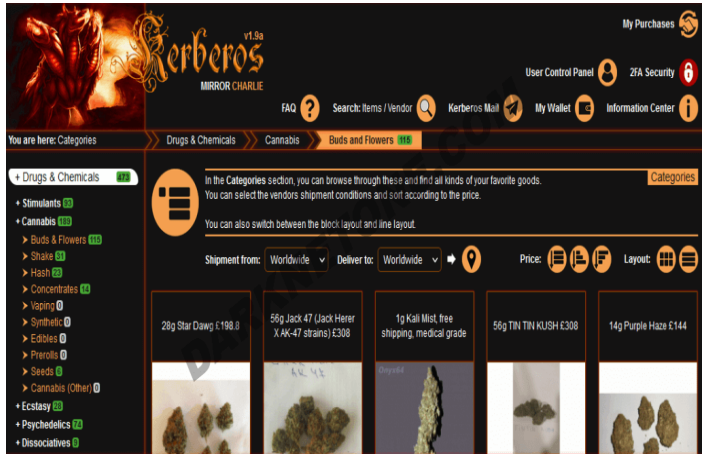












Copyright © 2023 CyberSecurity Malaysia

COMMUNICATION IN DARKWEB

TOX

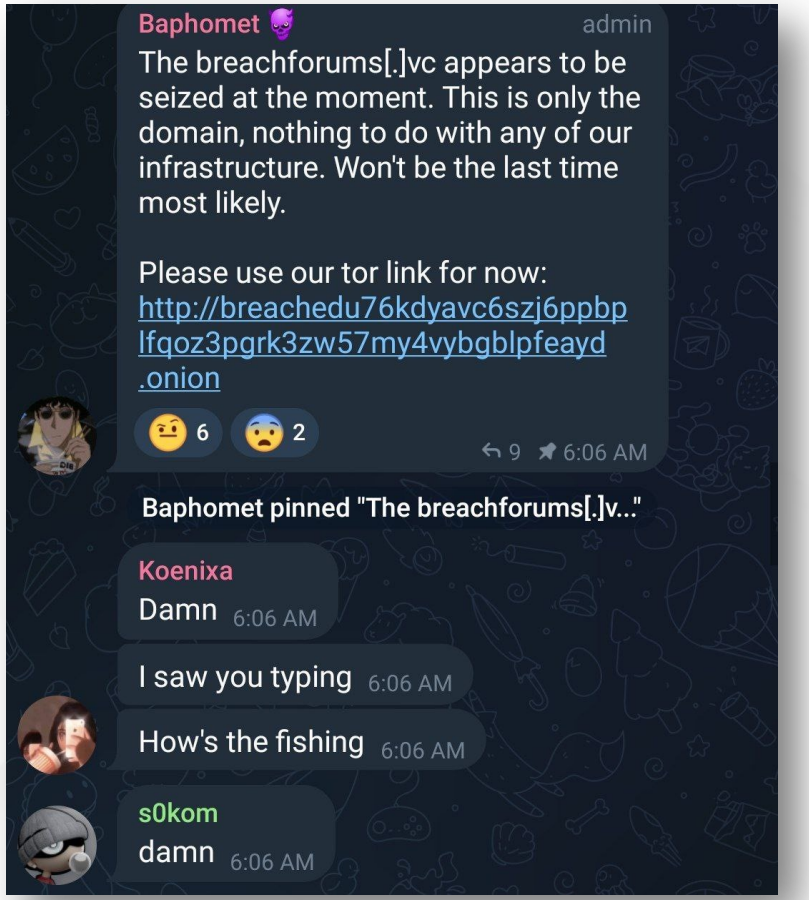
Telegram

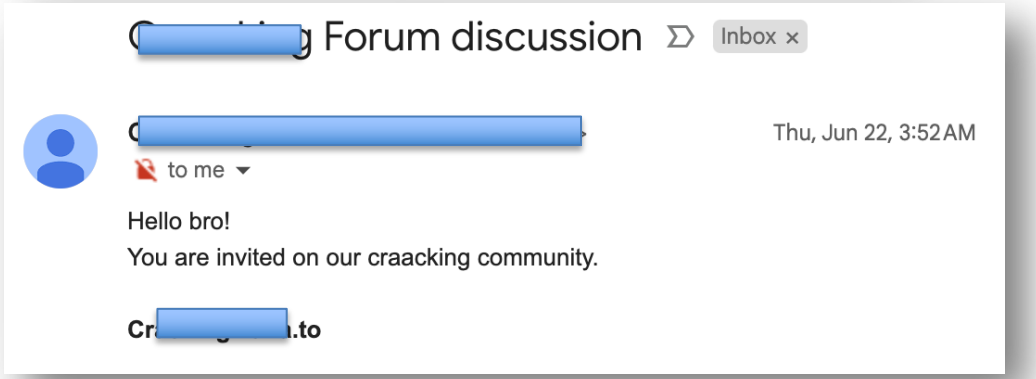
Discord

Proton Mail

Copyright © 2023 CyberSecurity Malaysia

COMMUNICATION IN DARKWEB





Copyright © 2023 CyberSecurity Malaysia

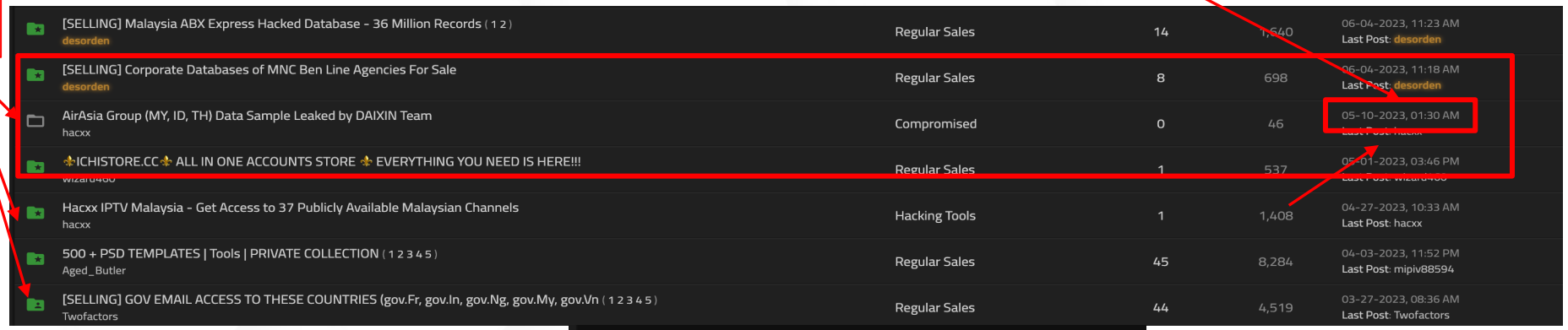
UNDERGROUND FORUM/MARKET

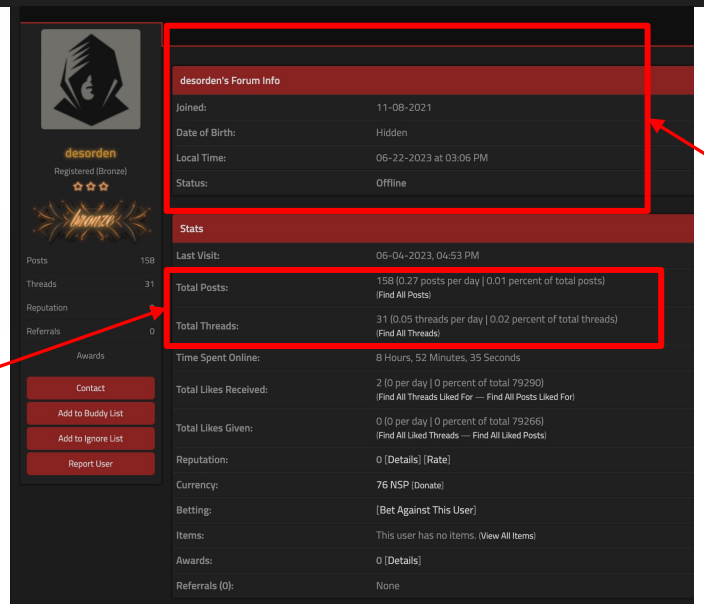
Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – SITE OVERVIEW (FORUM)

Threads in Subforum

Date + Time



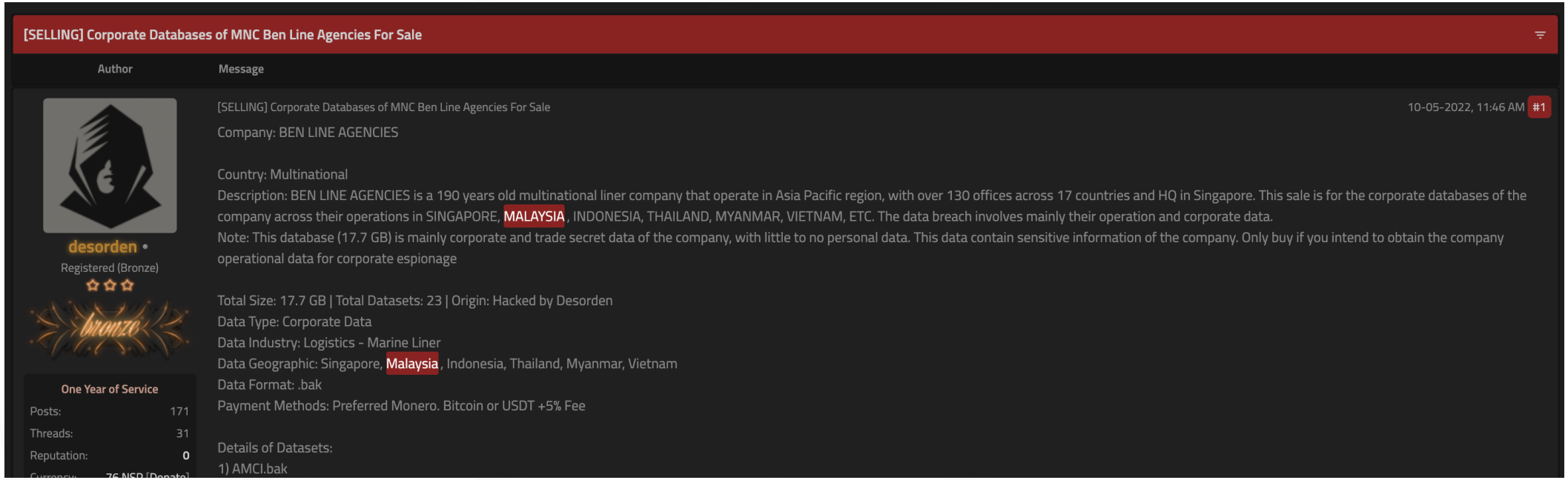


Post Content

User Information
(Joined date, # of posts, etc.)

Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – INCIDENT OVERVIEW



[SELLING] Corporate Databases of MNC Ben Line Agencies For Sale

Author	Message

desorden •
Registered (Bronze)

One Year of Service
Posts: 171
Threads: 31
Reputation: 0

[SELLING] Corporate Databases of MNC Ben Line Agencies For Sale — 10-05-2022, 11:46 AM #1

Company: BEN LINE AGENCIES

Country: Multinational
Description: BEN LINE AGENCIES is a 190 years old multinational liner company that operate in Asia Pacific region, with over 130 offices across 17 countries and HQ in Singapore. This sale is for the corporate databases of the company across their operations in SINGAPORE, MALAYSIA, INDONESIA, THAILAND, MYANMAR, VIETNAM, ETC. The data breach involves mainly their operation and corporate data.
Note: This database (17.7 GB) is mainly corporate and trade secret data of the company, with little to no personal data. This data contain sensitive information of the company. Only buy if you intend to obtain the company operational data for corporate espionage

Total Size: 17.7 GB | Total Datasets: 23 | Origin: Hacked by Desorden
Data Type: Corporate Data
Data Industry: Logistics - Marine Liner
Data Geographic: Singapore, Malaysia, Indonesia, Thailand, Myanmar, Vietnam
Data Format: .bak
Payment Methods: Preferred Monero. Bitcoin or USDT +5% Fee

Details of Datasets:
1) AMCI.bak

Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – SITE OVERVIEW (MARKET)

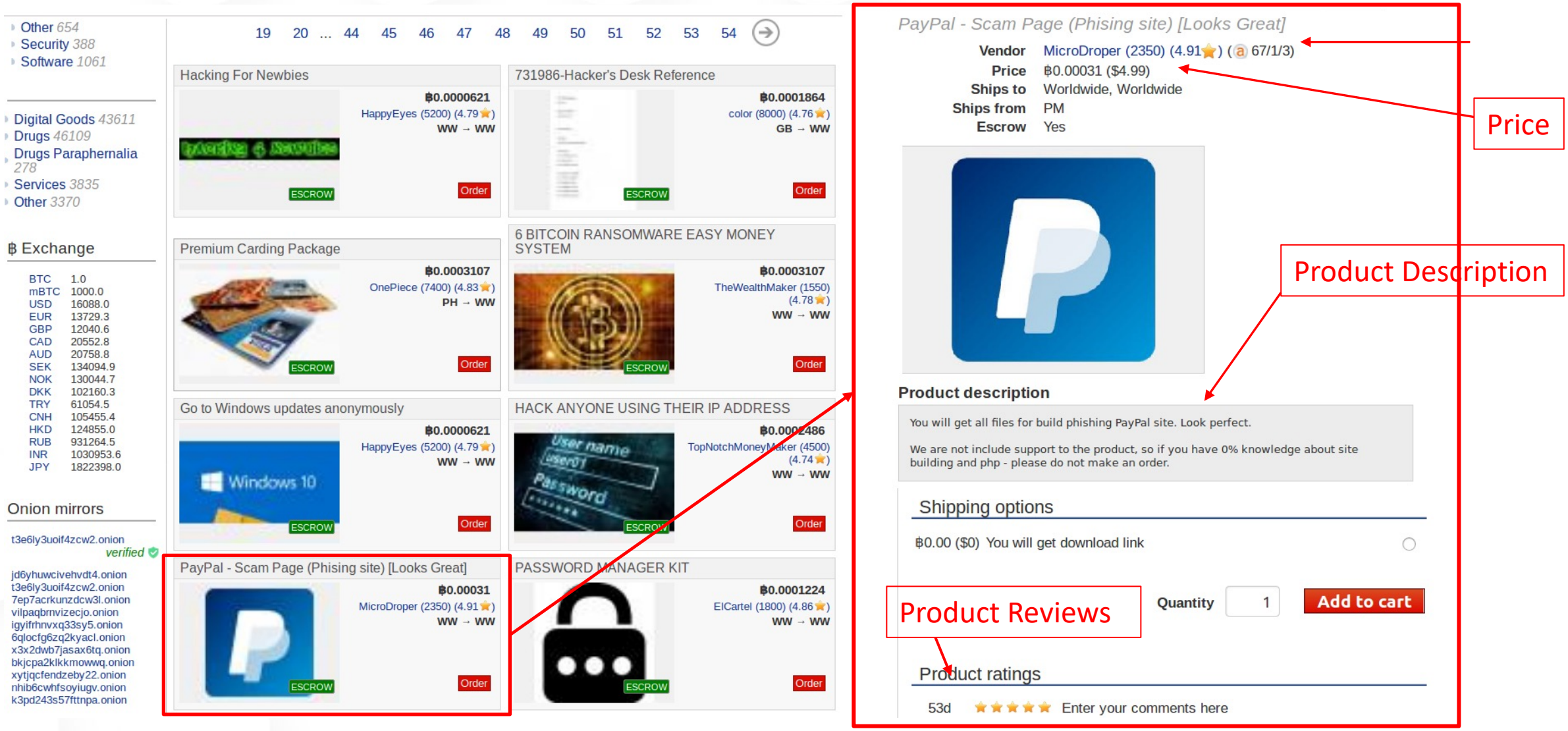


Figure 1. Snapshot of Dream Market and an Example of a Phishing Product for PayPal.

Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – SITE OVERVIEW (CARDING)

Search Functionality

Bank Identification Number

Credit Card Type

Expiration Date

Bank Name

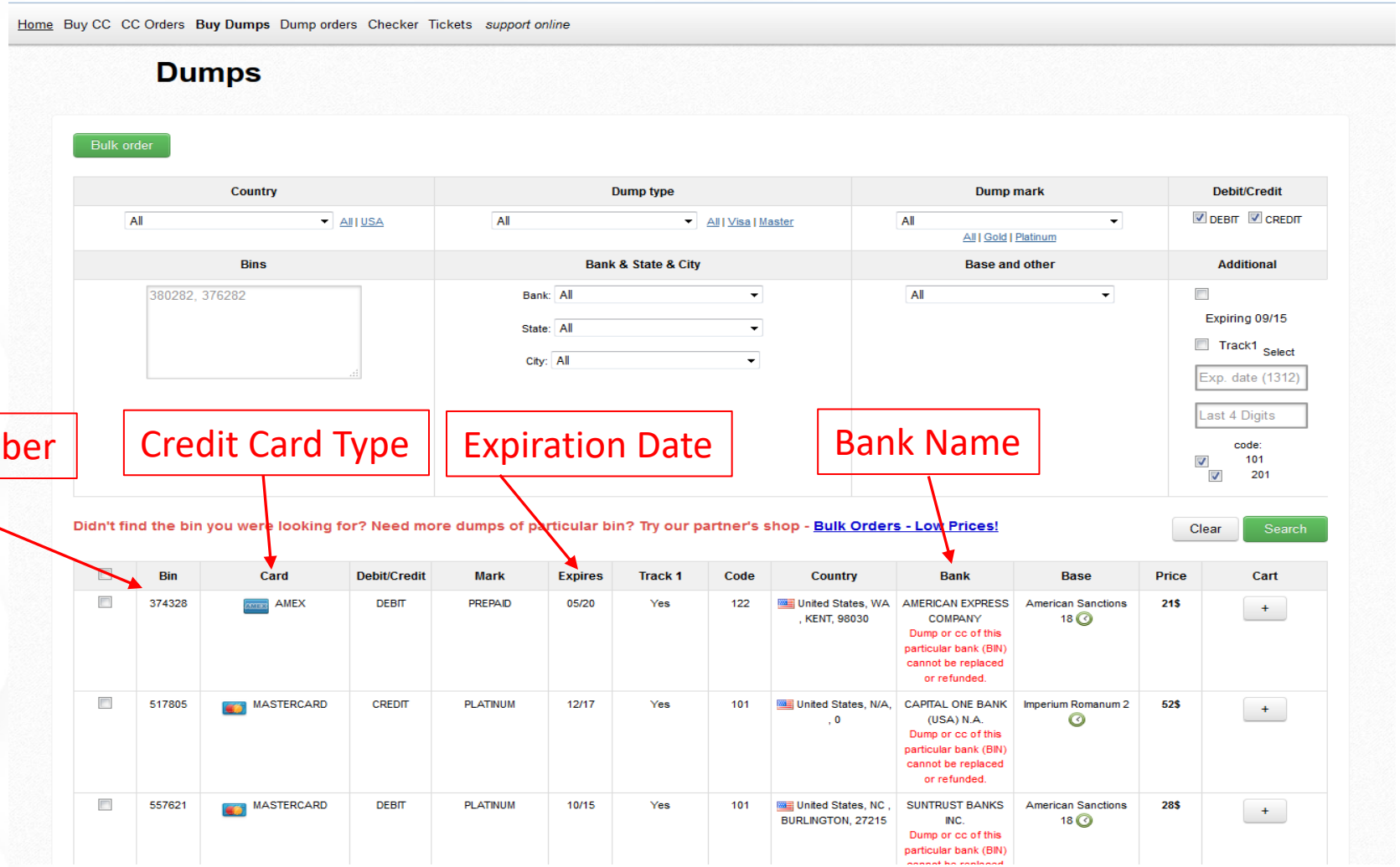


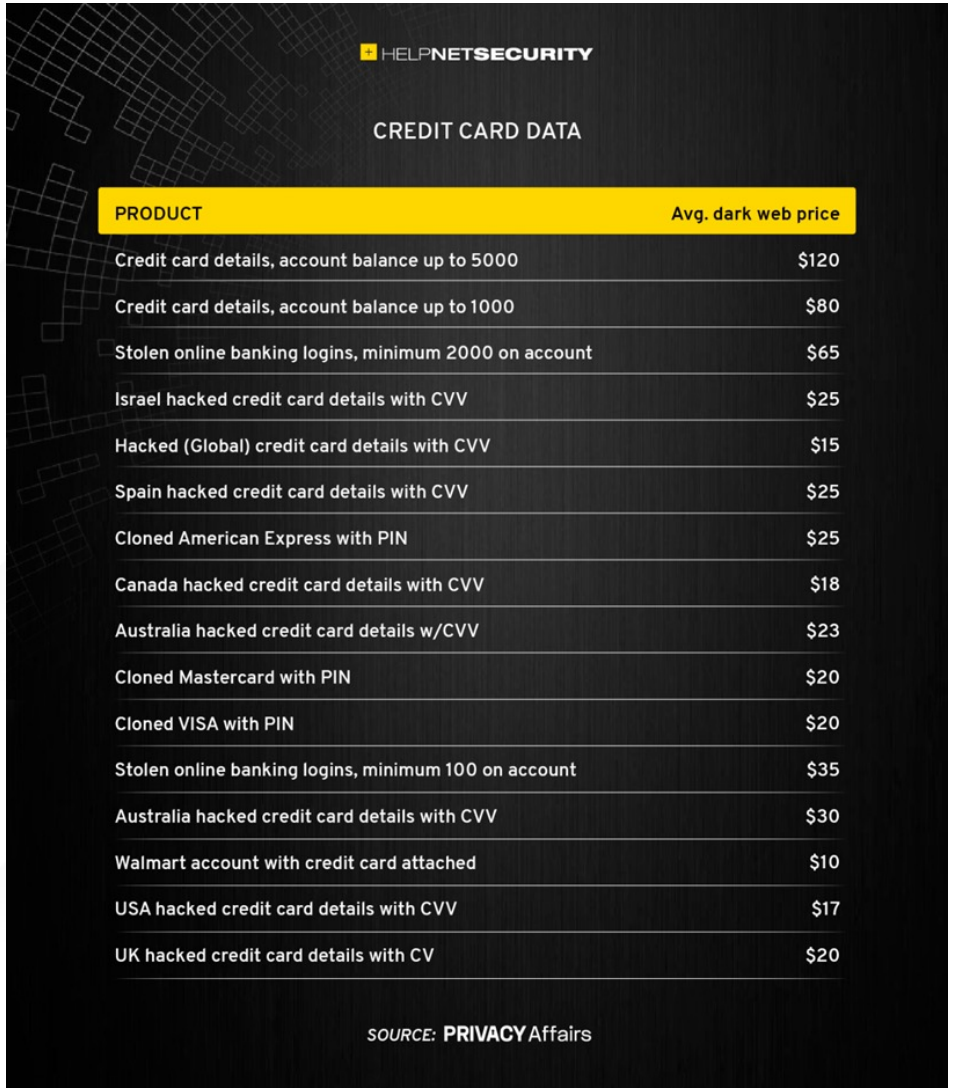
Figure 3. An Example of a Carding Shop Featuring Stolen Credit Cards

Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – CRYPTOCURRENCY

The Dark Web Price Index 2022 – based on data scanning dark web marketplaces, forums, and websites, revealed:

- Credit card details and associated information. Cost between $17-$120
- Online banking login information costs $45
- Hacked Facebook account: $45
- Cloned VISA with PIN: $20
- Stolen PayPal account details, minimum $1000 balances: $20.



HELPNETSECURITY

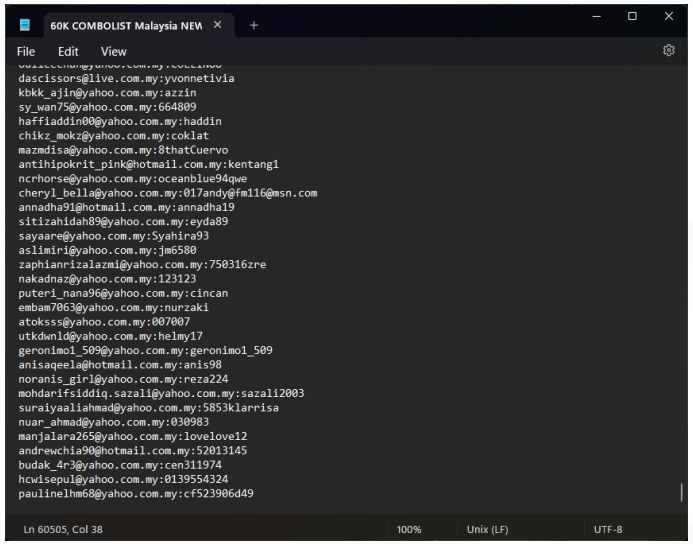
CREDIT CARD DATA

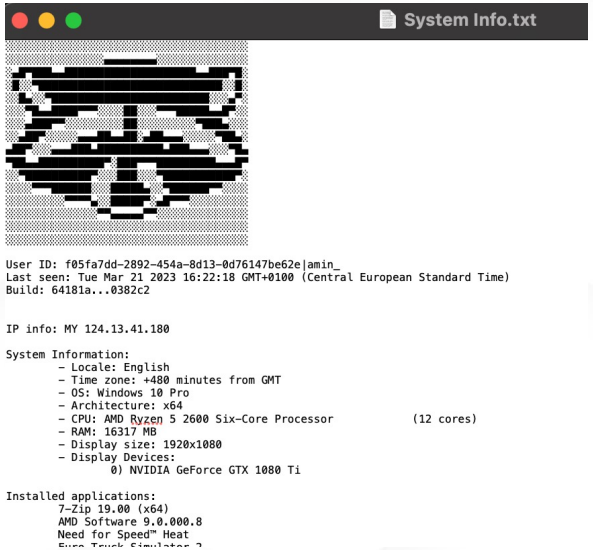
PRODUCT	Avg. dark web price
Credit card details, account balance up to 5000	$120
Credit card details, account balance up to 1000	$80
Stolen online banking logins, minimum 2000 on account	$65
Israel hacked credit card details with CVV	$25
Hacked (Global) credit card details with CVV	$15
Spain hacked credit card details with CVV	$25
Cloned American Express with PIN	$25
Canada hacked credit card details with CVV	$18
Australia hacked credit card details w/CVV	$23
Cloned Mastercard with PIN	$20
Cloned VISA with PIN	$20
Stolen online banking logins, minimum 100 on account	$35
Australia hacked credit card details with CVV	$30
Walmart account with credit card attached	$10
USA hacked credit card details with CVV	$17
UK hacked credit card details with CV	$20

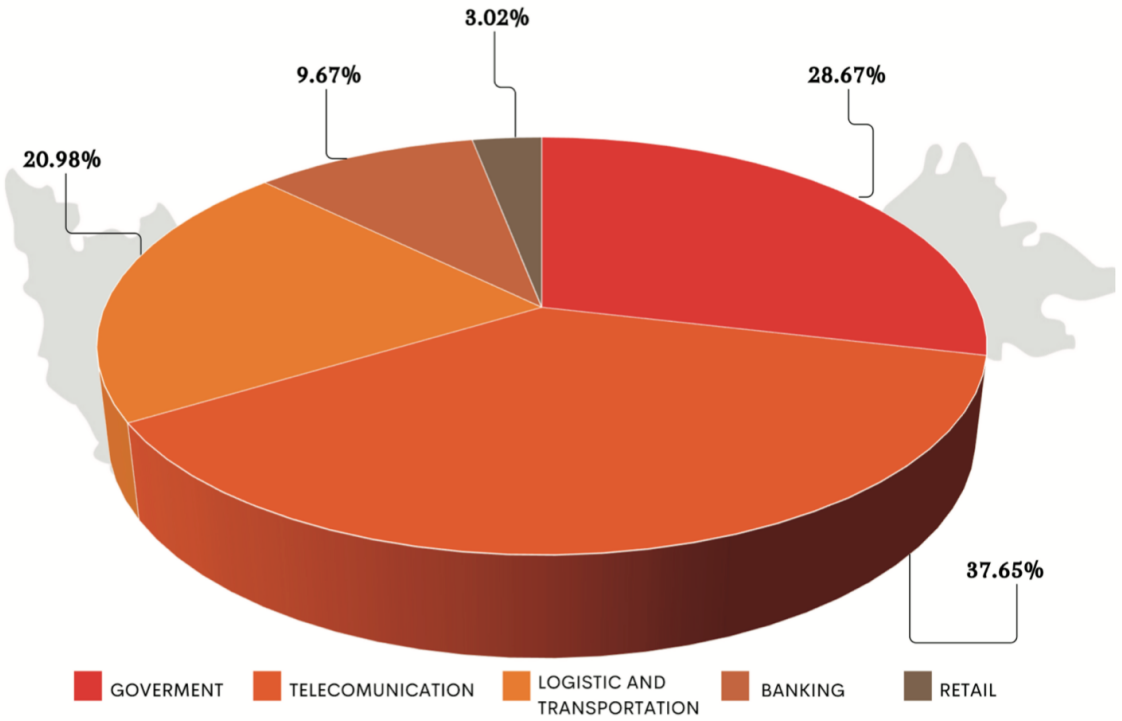
SOURCE: PRIVACY Affairs

Copyright © 2023 CyberSecurity Malaysia

CASE STUDY – SAMPLE DATA





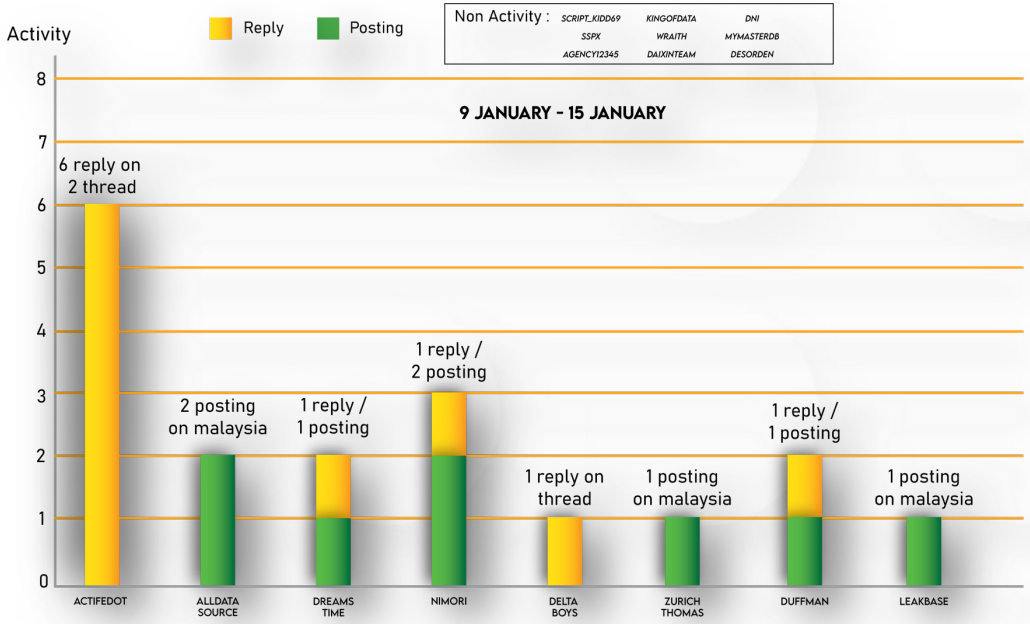


Total data leak in Q1 and Q2

Copyright © 2023 CyberSecurity Malaysia

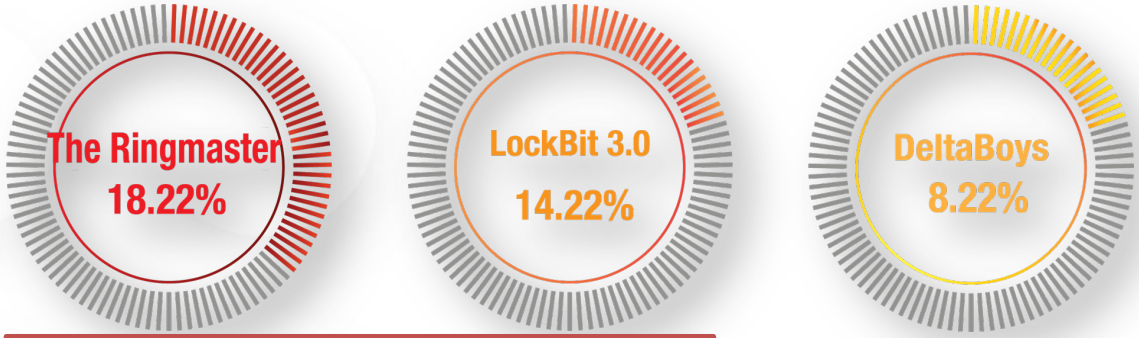
Visualization Finding Threat Actor Monitoring

1. Threat Actor Activity monitored by weekly



2. Total Threat Actor and Incident happened in Malaysia

3. Top 3 Active Threat Actor

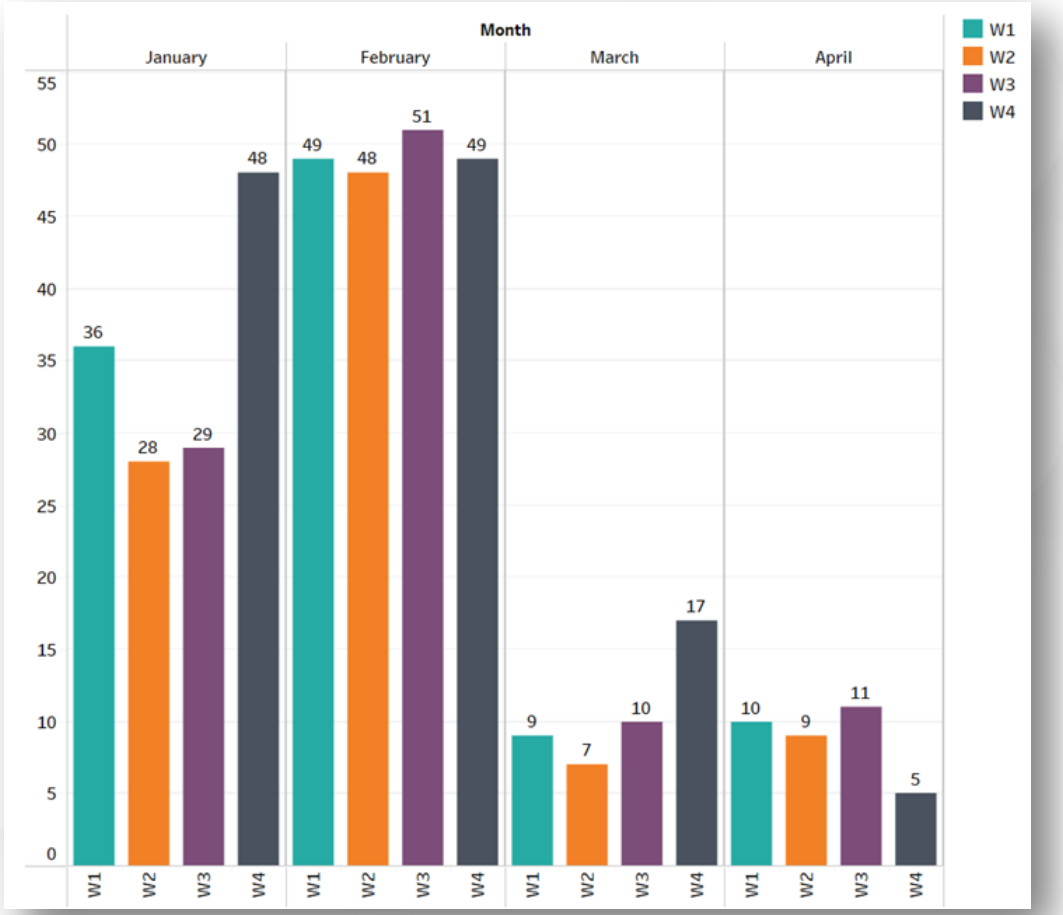


4. Timeline Threat Actor Activity by Weekly

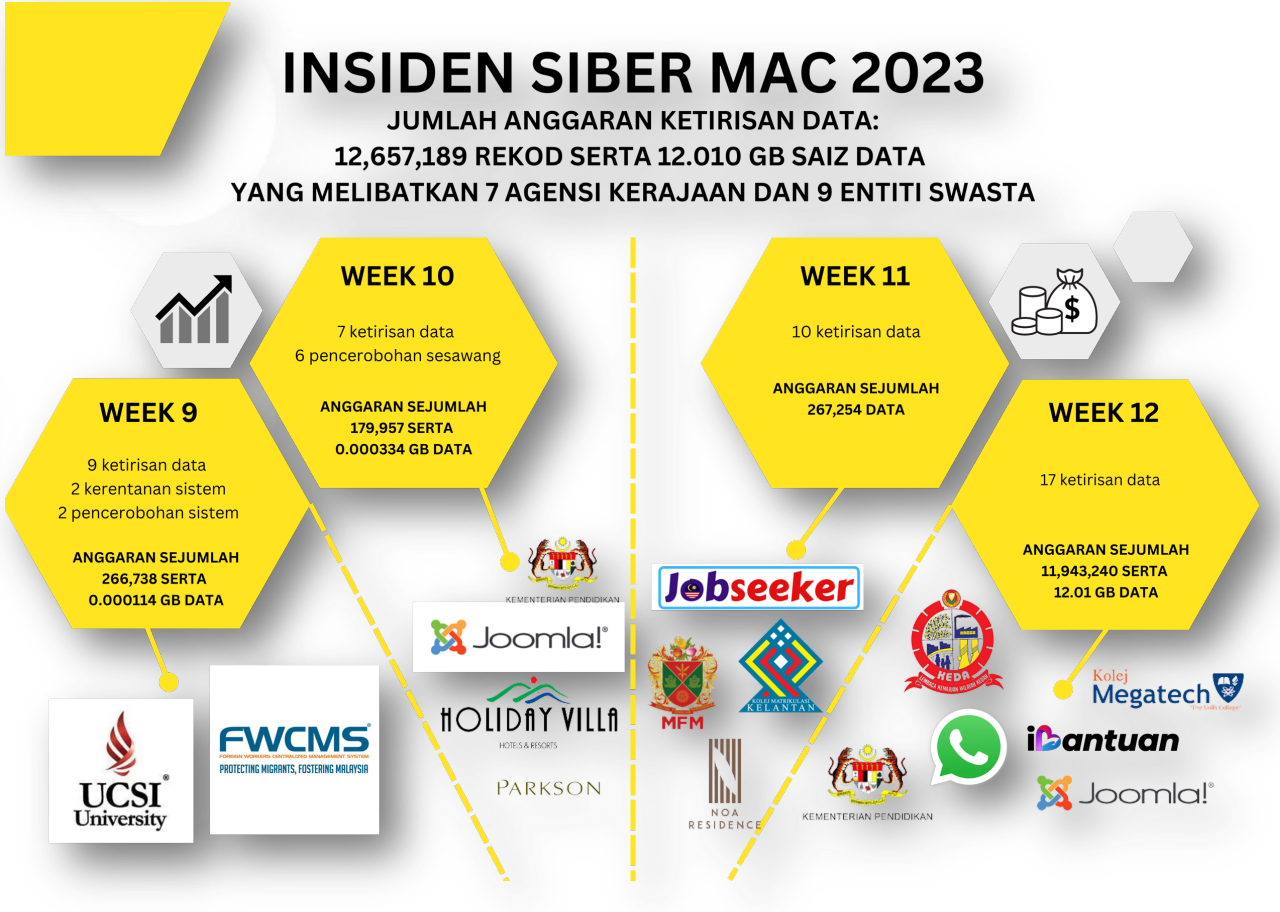
Copyright © 2023 CyberSecurity Malaysia

Incident Landscape in Malaysia

1. Graph trend for cyber incident happened in Malaysia.

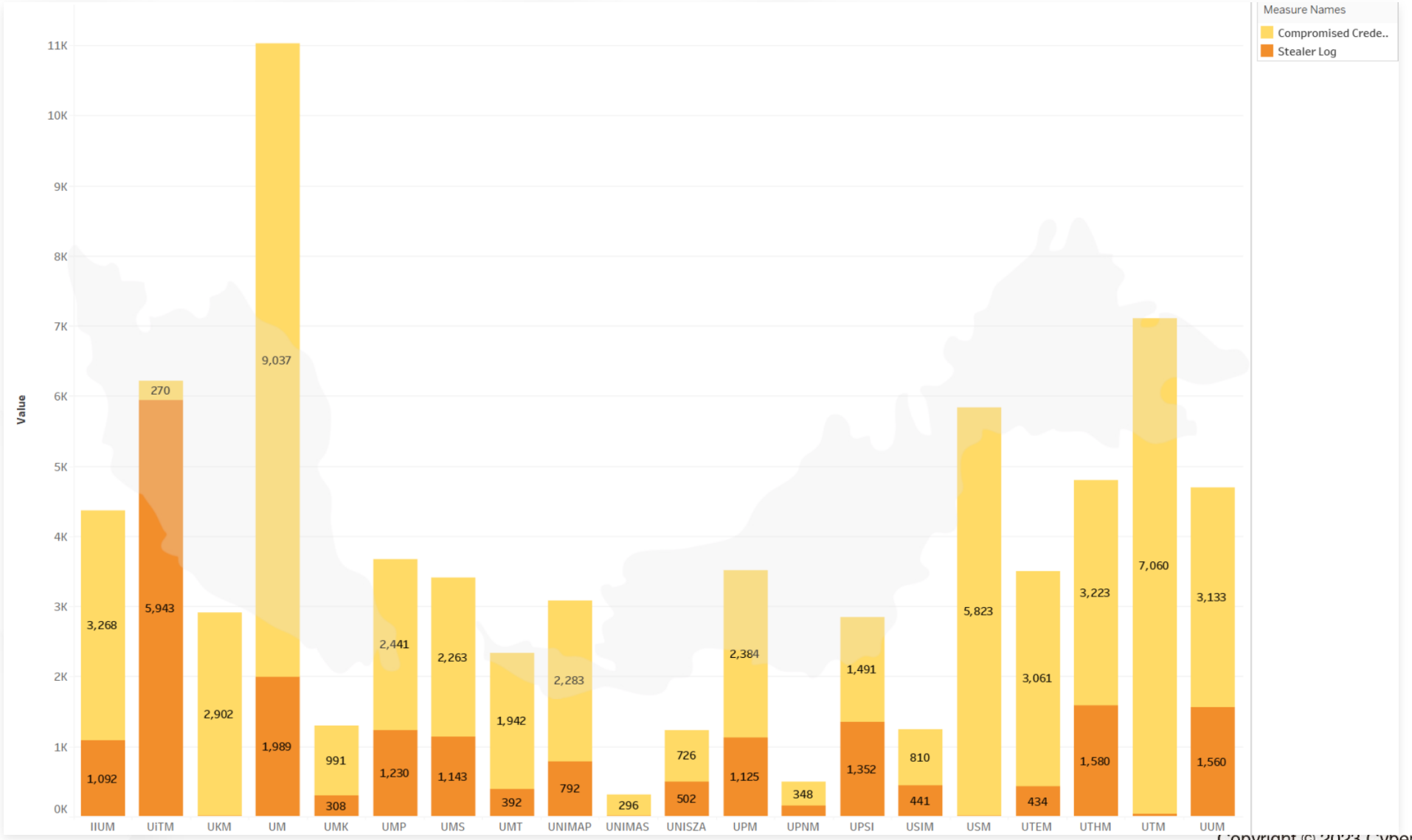


2. Infographic for summarizing cyber incident monthly.



Copyright © 2023 CyberSecurity Malaysia

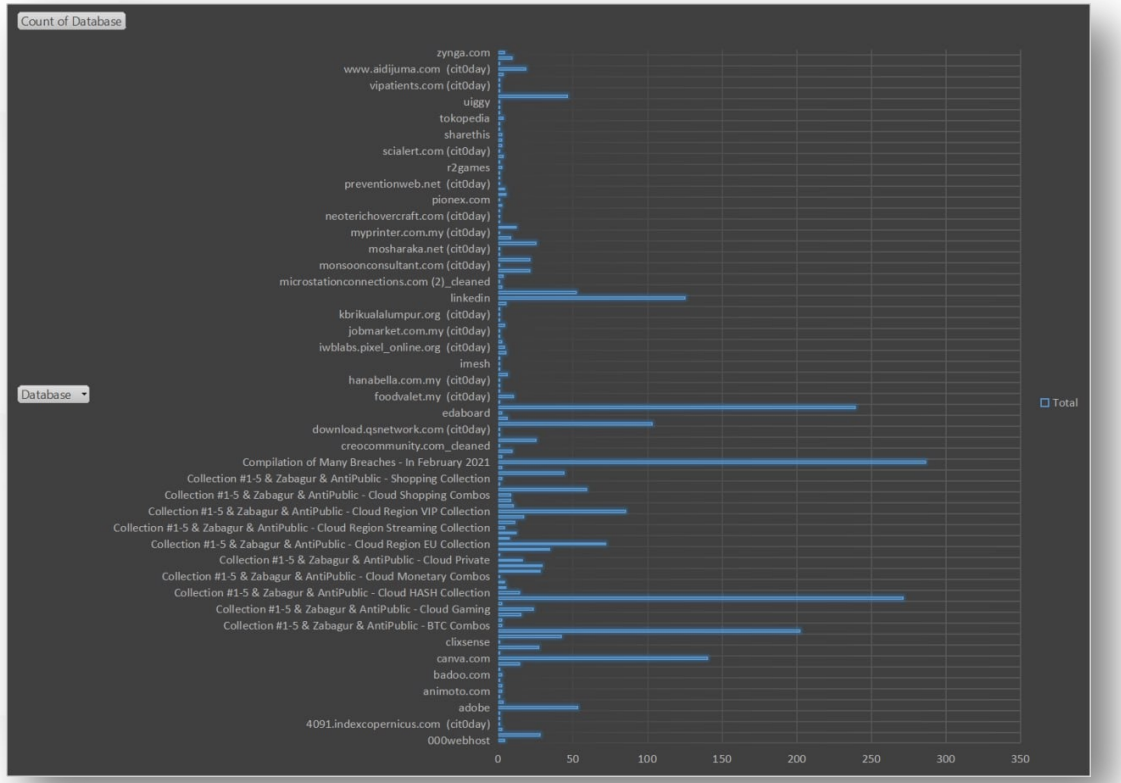
Dark Web Monitoring | IPTA



Copyright © 2023 CyberSecurity Malaysia

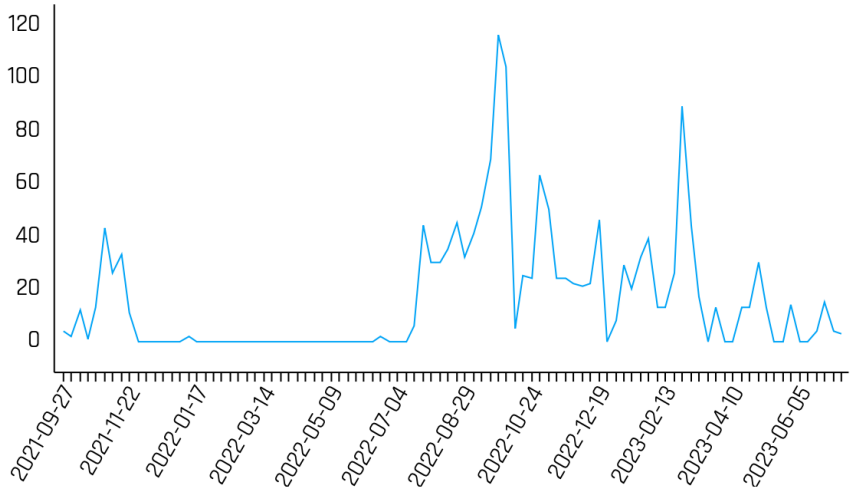
CASE STUDY – SAMPLE DATA (EDU.MY)

Date	Domain	Email	IP Address	Username	Password	Name	Vin
2023-	[redacted]	.edu.my	a[redacted]	u.my	[redacted]	mad_Mohamed_7	
2023-		.edu.my	s[redacted]	.my			
2023-		.edu.my	m[redacted]	du.my			
2023-		.edu.my	h[redacted]	.my			
2023-		.edu.my	f[redacted]	u.my			
2023-		.edu.my	f[redacted]	u.my	2602		
2023-		.edu.my	s[redacted]	p.edu.my	hna82		
2023-		.edu.my	c[redacted]	du.my			
2023-		.edu.my	n[redacted]	.edu.my			
2023-		.edu.my	r[redacted]	u.my			
2023-		.edu.my	h[redacted]	.edu.my			
2023-		.edu.my	n[redacted]	du.my			
2023-		.edu.my	n[redacted]	du.my	family		
2023-		.edu.my	m[redacted]	du.my			
2023-		.edu.my	f[redacted]	edu.my	5		
2023-		.edu.my	f[redacted]	my			
2023-		.edu.my	k[redacted]	du.my			
2023-		.edu.my	e[redacted]	np.edu.my			
2023-		.edu.my	a[redacted]	u.my			
2023-		.edu.my	fi[redacted]	y			
2023-		.edu.my	a[redacted]	du.my			
2023-		.edu.my	m[redacted]	.my			
2023-		.edu.my	fe[redacted]	my			
2023-		.edu.my	a[redacted]	edu.my			
2023-		.edu.my	li[redacted]				
2023-		.edu.my	c[redacted]	my			
2023-		.edu.my	h[redacted]	my			
2023-		.edu.my	w[redacted]	u.my			
2023-		.edu.my	zi[redacted]	y			
2023-		.edu.my	k[redacted]	my			
2023-		.edu.my	a[redacted]	np.edu.my	5774		
2023-		.edu.my	r[redacted]	my		Rosshalila Sharip	
2023-		.edu.my	s[redacted]	du.my			



Copyright © 2023 CyberSecurity Malaysia

THREAT ACTOR PROFILING



TIMELINE FOR INDICATED TIMEFRAME

forum_breached	77%
forum_sinisterly	12%
forum_raidforum	6%
forum_breach	1%
forum_cracked	1%
forum_nulledbb	1%
forum_nulled	1%
telegram	1%

STATISTIC SITE THREAT ACTOR REGISTERED

Data_leak	22%
Download_link	12%
Bitcoin	11%
Cryptocurrency	11%
Hacking	10%
Email_address	10%
email	10%
Email_domain	6%
Drugs	4%
Fraud	4%

STATISTIC ACTICITIES OF THREAT ACTOR IN THE FORUM

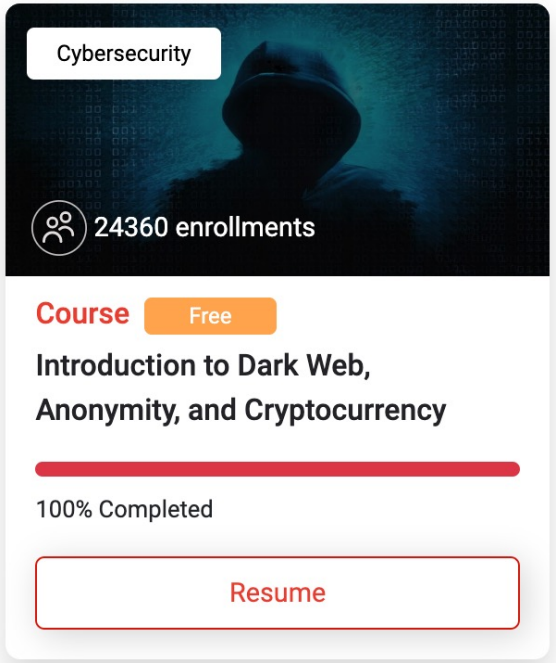
Copyright © 2023 CyberSecurity Malaysia

THREAT ACTOR PROFILING

Copyright © 2023 CyberSecurity Malaysia

DARKWEB CERTIFICATE

Introduction to Dark Web, Anonymity, and Cryptocurrency



SOURCE: https://codered.eccouncil.org/course/introduction-to-dark-web-anonymity-and-cryptocurrency

Copyright © 2023 CyberSecurity Malaysia

MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity MALAYSIA

THANK YOU

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia

T +603 8800 7999 | **F** +603 8008 7000 | **H** +61 300 88 2999

www.cybersecurity.my | info@cybersecurity.my

CyberSecurityMalaysia | cybersecuritymy | cybersecuritymy | CyberSecurity Malaysia | cybersecurity_my

JUBLI PERAK 1997 - 2022 CyberSecurity MALAYSIA

SIBER MALAYSIA MADANI

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB 021
SAMM 456

MSC MALAYSIA Status Company

WSIS PRIZES 2020 WINNER www.wsis.org

THE MALAYSIA BOOK of RECORDS

Copyright © 2023 CyberSecurity Malaysia